Chapter 8

The Sylow Theorems

Introduction

Lagrange's Theorem tells us that in any finite group G the order of a subgroup H divides the order of G. However, the theorem says nothing about the *existence* of the subgroups of the possible orders: indeed, we know that G may fail to have a subgroup corresponding to some divisors of its order. For example, the alternating group A_4 of order 12 has no subgroup of order 6. However, we will show that there is a subgroup corresponding to every *prime power* divisor of the order of the group. This theorem will be the main result of this chapter. It ensures that, for example, a group of order

$$24 = 8 \times 3 = 2^3 \times 3$$

has subgroups of orders 2, 2^2, 2^3 and 3.

Any subgroup whose order is the highest power of a particular prime dividing the order of the group has additional properties that can be of assistance in classifying the groups of a given order. For example, the theorems that we prove will enable us to say that any group of order $91 = 7 \times 13$ must have a normal subgroup of order 13. This, in turn, will enable us to show that any group of order 91 is cyclic.

For a group of order 24, 2^3 is the highest power of 2 dividing the order.

Broadly speaking, the results that we will prove guarantee the existence of subgroups corresponding to prime power divisors of the order of a group and provide restrictions on the number of such subgroups a group can possess.

These results are due to the Norwegian mathematician L. Sylow (1832–1918). The original proofs start by considering the special case of abelian groups. However, the tools provided by group actions give more concise proofs, and these are the proofs we give.

The name Sylow is usually pronounced as 'Seeloff' or 'Seelow'.

The first section of this chapter introduces and proves these important results. In Subsection 1.1, we introduce a new group action and investigate its application to some particular examples. These examples will point the way to the general results that are needed. The use of group actions requires us to know the number of elements in the set being acted on. In the actions that we use, this involves knowledge of certain binomial coefficients.

Subsection 1.2 generalises the special cases of Subsection 1.1 to provide a proof of the first two of the Sylow Theorems.

Subsection 1.3 completes the proofs of Sylow's results with a proof of his third theorem.

In Section 2, we apply the results obtained to finite abelian groups and to other groups of various orders.

Section 3 shows that some of the results generalise to any prime power divisor of the order of a group.

The final section of this chapter and this book starts with a series of exercises that pulls together many of the ideas we have covered so far in

Book B in order to find all the possible groups of order $2p^2$, where p is an odd prime.

Chapter guide

Section 1 is a rather long one, with three subsections of roughly equal length in terms of study time. Section 2 consists mainly of exercises and thus will require a similar amount of study time in spite of being shorter. In compensation, Sections 3 and 4 are rather shorter.

The theorems proved in this chapter are powerful, general ones. It follows that some of the work, in Subsection 1.2 and Section 3 in particular, is fairly theoretical. The proofs in these sections are pivotal in the development of the theory of finite groups. In this chapter, we are also interested in using these theorems to determine the structure of particular groups, and the exercises in Section 2 have been designed with this aim in mind. The exercises in Section 4 require results from the whole of Book B, so they will be useful for revision.

1 The Sylow Theorems

The Sylow Theorems are a series of powerful results that give a wealth of information about the possible orders and number of subgroups of a finite group. In particular, Sylow's First Theorem provides a partial converse to Lagrange's Theorem.

1.1 Sylow p-subgroups

In Chapter 6 we proved Cauchy's Theorem (Theorem 3.16), which states that if a finite group G has order n and a prime number p divides n, then G has a subgroup of order p. The main aim of this chapter is to establish the Sylow Theorems, the first of which is an extension of Cauchy's Theorem.

Theorem 1.1 *Sylow's First Theorem*

Let G be a finite group of order n and let p be a prime dividing n, where p^α is the highest power of p dividing n. Then G has a subgroup of order p^α.

The proof of this theorem is postponed until Subsection 1.2.

The subgroup of order p^α in the statement of the theorem is called a **Sylow p-subgroup** of G, and the divisor p^α of n, which is the largest power of p that divides n, is referred to as the **maximal prime power divisor** corresponding to p.

For example, the theorem tells us that the permutation group S_4, which has order $4! = 24$, has subgroups of orders $2^3 = 8$ and 3.

From Theorem 4.3 of Chapter 7, we know that a p-group has subgroups corresponding to every divisor of its order. Taken together with Sylow's First Theorem, this means that a finite group has a subgroup corresponding to *every* prime power divisor of its order. As this result is sometimes useful, we state it as a corollary.

Corollary 1.2

Let G be a finite group of order n and let p be a prime dividing n. If p^k divides n then G has a subgroup of order p^k.

Hence the permutation group S_4 has subgroups of orders 2 and $2^2 = 4$ as well as the ones mentioned above.

In Example 1.3 we illustrate the structure of the proof of Sylow's First Theorem by considering a specific example, and we introduce the group action that we will use later to prove the theorem. The group action we want is a generalisation of the action of a group on itself by left multiplication.

Example 1.3 *Subgroups of a group of order 20*

Let G be any group of order $20 = 2^2 \times 5$. The order of G is divisible by the primes 2 and 5. The maximal prime power divisors of $|G|$ corresponding to 2 and 5 are $2^2 = 4$ and $5^1 = 5$, respectively.

We show that G must have a subgroup of order 4.

Let X be the collection of all four-element subsets of G. We define an action of the group G on the set X by

$$g \wedge A = gA = \{ga : a \in A\}$$

for every element A of X.

Note that this is different from our proof of Cauchy's Theorem, where the set acted upon consisted of tuples of elements rather than subsets. Since these are subsets, the four elements are distinct.

Thus, G acts on X by left multiplication.

In order to verify that we have indeed defined a group action according to Definition 3.1 of Chapter 6, we must show that $g \wedge A$ is an element of X for all $g \in G$ and $A \in X$, and that:

(a) $e \wedge A = A$ for all $A \in X$

(b) $(gh) \wedge A = g \wedge (h \wedge A)$ for all $g, h \in G$ and $A \in X$.

So that we do not break the flow of the example, we ask you to check that this is an action in a more general case in Exercise 1.2 below.

As for any group action, we can immediately make two statements. One comes from the fact that the orbits partition X; the other comes from the Orbit–Stabiliser Theorem, that is, Corollary 3.13 of Chapter 6.

Suppose that $\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$ are the distinct orbits for this group action. We know these orbits partition X, so

$$|X| = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

We call this the **partition equation**. By the Orbit–Stabiliser Theorem,

$$|G| = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)|, \quad i = 1, \ldots, s.$$

Since we are searching for a subgroup of order 4, we could show that one of the four-element subsets that are the elements of X must be a subgroup of G. Alternatively, we could show that one of the stabilisers, which we know are subgroups of G, must have four elements. Both approaches are possible; we choose the second.

To make use of the equations above, we need to know $|X|$, the size of X. Since G has 20 elements, the number of four-element subsets of G is the number of ways of choosing four elements from 20, that is,

The **binomial coefficient** ${}^nC_r$ can be calculated from
$${}^nC_r = \frac{n!}{r!(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r!}.$$

$$\begin{aligned} {}^{20}C_4 &= \frac{20 \times 19 \times 18 \times 17}{4 \times 3 \times 2 \times 1} \\ &= \frac{5 \times 19 \times 9 \times 17}{1 \times 3 \times 1 \times 1} \\ &= 5 \times 19 \times 3 \times 17 \\ &= 4845. \end{aligned}$$

Hence $|X| = 4845$ and the partition equation is

$$4845 = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

The Orbit–Stabiliser Theorem gives

$$20 = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)|, \quad i = 1, \ldots, s.$$

We will use these equations to deduce that there is a stabiliser whose order is 4. By the Orbit–Stabiliser Theorem, the orbit corresponding to such a stabiliser has size 5, which is not divisible by 2. This observation prompts us to look for an orbit whose size is not divisible by 2.

If all the terms in the sum on the right-hand side of the partition equation were divisible by 2, then so would be the left-hand side. But the left-hand side, 4845, is *not* divisible by 2, so we can deduce that at least one of the terms

$$|\mathrm{Orb}(A_1)|, |\mathrm{Orb}(A_2)|, \ldots, |\mathrm{Orb}(A_s)|$$

on the right-hand side is not divisible by 2. Therefore there is an element A of X such that

$$|\mathrm{Orb}(A)|$$

is not divisible by 2.

Applying the Orbit–Stabiliser Theorem to A gives

$$|G| = 20 = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Since $|\mathrm{Orb}(A)|$ is not divisible by 2 and $|G|$ is divisible by 4, it follows that $|\mathrm{Stab}(A)|$ is divisible by 4. From this we deduce that

$$|\mathrm{Stab}(A)| \geq 4.$$

So far we have established the existence of a *subgroup* $\mathrm{Stab}(A)$ of G of order at least 4. If we could show that $|\mathrm{Stab}(A)| \leq 4$, the proof would be complete.

So far we have used the partition equation of the group action and the Orbit–Stabiliser Theorem, but not the fact that the elements of X are subsets of the group G. We will now exploit this fact as we inspect carefully the consequences of the definition of a stabiliser.

Suppose that g is any element of $\mathrm{Stab}(A)$. Then $g \wedge A = A$. Now choose a fixed element a in A. Since our action is defined by left multiplication, we have

$$ga \in g \wedge A = A.$$

So $ga \in A$ for every element g in $\mathrm{Stab}(A)$.

If we consider all the elements of the form ga, for g in $\mathrm{Stab}(A)$, we obtain the right coset

$$\mathrm{Stab}(A)a$$

of $\mathrm{Stab}(A)$. We have just shown that all elements of this right coset are in A. Hence

$$\mathrm{Stab}(A)a \subseteq A.$$

Thus, $\mathrm{Stab}(A)a$ cannot have more elements than A, and so

$$|\mathrm{Stab}(A)a| \leq |A| = 4.$$

However, right cosets have the same number of elements as the subgroup from which they are formed. Thus

$$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq 4.$$

This provides the other inequality that we wanted and we deduce that

$$|\mathrm{Stab}(A)| = 4.$$

We have shown the existence of a subgroup $\mathrm{Stab}(A)$ of G that has order 4, as required.

Thus, we have shown that any group G of order 20 has a Sylow 2-subgroup of order 4.

Exercise 1.1

Adapt the argument used in Example 1.3 to show that any group of order 20 must have a Sylow 5-subgroup of order 5. You should define an appropriate group action, but you need not prove that it is an action.

To complete the arguments used in Example 1.3 and in the solution to Exercise 1.1, we need to prove that the group actions we defined are indeed actions. You are asked to do this in the next exercise.

Exercise 1.2

Let G be a finite group and let X be the set of all subsets of G that have exactly k elements. Define

$$g \wedge A = gA$$

for every $g \in G$ and $A \in X$.

Show that this defines an action of G on X by proving that $g \wedge A$ is an element of X, that is, it is a k-element subset, and that for all $g, h \in G$ and $A \in X$:

(a) $e \wedge A = A$

(b) $(gh) \wedge A = g \wedge (h \wedge A)$.

We now examine the key steps in Example 1.3 and in the solution to Exercise 1.1 to see what we need to do to generalise the proofs.

Suppose that G is a group of order n, that p is a prime that divides n, and that p^α is the highest power of p that divides n. In this setting, the key steps in Example 1.3 and Exercise 1.1 generalise as follows.

1. Define X to be the set consisting of all subsets of G containing p^α elements.
2. Define an action of G on X by left multiplication, that is,

   $$g \wedge A = gA, \quad g \in G,\ A \in X.$$

   The solution to Exercise 1.2 ensures that this *is* a group action.
3. Show that $|X|$ is not divisible by p.
4. Suppose that $\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$ are the distinct orbits for this group action and deduce from the partition equation

   $$|X| = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|$$

   that at least one orbit has order not divisible by p.
5. If A is an element in X such that $|\mathrm{Orb}(A)|$ is not divisible by p, use the Orbit–Stabiliser Theorem

   $$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|$$

   to deduce that $|\mathrm{Stab}(A)|$ is divisible by p^α. Hence

   $$|\mathrm{Stab}(A)| \geq p^\alpha.$$
6. Show that, for a fixed element a of A,

   $$\mathrm{Stab}(A)a \subseteq A$$

   and, hence, that

   $$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = p^\alpha.$$

   Since both $\mathrm{Stab}(A)a$ and A have p^α elements and $\mathrm{Stab}(A)a \subseteq A$, we have $\mathrm{Stab}(A)a = A$.
7. Conclude that $\mathrm{Stab}(A)$ has p^α elements and so it is a subgroup of G of order p^α.

We can extract three results from the above proof strategy that it is useful to summarise in the following lemma. The proofs of parts (a) and (b) are given after the proof of Sylow's First Theorem, in Subsection 1.2. The proof of part (c) follows directly from the marginal note next to step 7 above.

Lemma 1.4

Let G be a finite group and let X be the set of all the k-element subsets of G. If G acts by left multiplication on X and if $A \in X$, then:

(a) $|\mathrm{Stab}(A)|$ divides $|A|$.

(b) If k is a power of a prime p, then $\mathrm{Stab}(A)$ is a p-group.

(c) If k is the maximal power of p dividing the order of G and if p does not divide $|\mathrm{Orb}(A)|$, then

$$\mathrm{Stab}(A)a = A \quad \text{for any } a \in A.$$

In Example 1.3 we could replace the order of the group, 20, with a general value n, and the prime 2 with a general prime p, throughout, and still have a valid proof except at one point. One crucial step involved observing that the number of elements of X was not divisible by 2. For a general proof we would have to show the corresponding statement that if p^α is the highest power of p dividing the order of the group, then the number of p^α-element subsets of the group is not divisible by p. That is, we would have to show that the binomial coefficient ${}^nC_{p^\alpha}$ is not divisible by p.

We will consider such divisibility properties of binomial coefficients in Subsection 1.2. Once we have shown that ${}^nC_{p^\alpha}$ is not divisible by p, the discussion above shows that all the other steps in the argument do generalise and so give a proof of Sylow's First Theorem.

Exercise 1.3

(a) Show that ${}^{24}C_3$ is not divisible by 3, and hence that any group of order 24 has a subgroup of order 3.

(b) Show that any group of order 24 has a subgroup of order 8.

(c) Let G be a group of order 15. Show that G has a subgroup H of order 3 and a subgroup K of order 5.

The solution to Exercise 1.3 is quite instructive, in that the details of the calculations in parts (a) and (b) give some indication of why the binomial coefficient ${}^{24}C_3$ is not divisible by 3 and why the binomial coefficient ${}^{24}C_8$ is not divisible by 2. In the first case, the only term in the numerator divisible by 3 is 24, and its factor of 3 cancels with the corresponding term 3 in the denominator. In the second case, every term in the original numerator divisible by a power of 2 has a corresponding term in the denominator divisible by the same power of 2. Also note that in the

solution to part (c), the cancellations occur in corresponding terms as in the previous solutions.

The second and third Sylow Theorems, which we discuss later in this chapter, are concerned with the number of different Sylow p-subgroups corresponding to the prime p. To conclude this subsection, we investigate an example that indicates the nature of these results and which leads to a formulation of Sylow's Second Theorem.

Example 1.5 *Sylow 5-subgroups in groups of order 15*

We continue the investigation of groups of order 15, using the same notation as in Exercise 1.3(c).

Let G be a group of order 15, let X be the set of all five-element subsets of G and let

$$\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s)$$

be the distinct orbits under the action of G on X by left multiplication.

Since the Sylow 5-subgroups contain five elements, they are elements of X. Thus each 5-subgroup must be contained in some orbit of the action. We claim that the orbits that contain these subgroups are precisely the ones whose size is not divisible by 5, and that each such orbit contains exactly one Sylow 5-subgroup. Thus, counting the number of Sylow 5-subgroups is the same as counting the number of orbits whose size is not divisible by 5.

Our claim will be proved in the following three steps.

1. If $A \in X$ is such that 5 does not divide $|\mathrm{Orb}(A)|$, then $\mathrm{Orb}(A)$ contains a Sylow 5-subgroup.
2. If $\mathrm{Orb}(A)$ contains a Sylow 5-subgroup then 5 does not divide $|\mathrm{Orb}(A)|$.
3. Any orbit can contain at most one Sylow 5-subgroup.

Let us now go through each step.

1. If 5 does not divide $|\mathrm{Orb}(A)|$, we know from the proof strategy of Sylow's First Theorem that $\mathrm{Stab}(A)$ is a Sylow 5-subgroup. Call this subgroup H.

   Let $a \in A$. Then by Lemma 1.4 we have

   $$Ha = A.$$

   Now the orbit of A includes

   $$a^{-1} \wedge A = a^{-1}A = a^{-1}Ha.$$

   But $a^{-1}Ha$ is the conjugate of H by a^{-1}, and so it is a subgroup of G with the same order as H. This is because whenever H is a subgroup of a group G and $g \in G$, then gHg^{-1} is also a subgroup of G of the same order as H.

   Therefore $a^{-1}Ha$ is a Sylow 5-subgroup contained in $\mathrm{Orb}(A)$.

2. Suppose that $\mathrm{Orb}(A)$ contains the Sylow 5-subgroup H. This means that $\mathrm{Orb}(H) = \mathrm{Orb}(A)$.

   In order to show that $|\mathrm{Orb}(A)|$ is not divisible by 5, we show that $\mathrm{Stab}(H) = H$ and use the Orbit–Stabiliser Theorem.

   Let $g \in G$. Then

   $$g \wedge H = gH.$$

   Now $gH = H$ if, and only if, $g \in H$. That is, $g \in \mathrm{Stab}(H)$ if, and only if, $g \in H$. Thus $\mathrm{Stab}(H) = H$.

   The Orbit–Stabiliser Theorem gives

   $$|G| = 15 = |\mathrm{Orb}(H)| \times |\mathrm{Stab}(H)| = |\mathrm{Orb}(H)| \times 5.$$

   This shows that $|\mathrm{Orb}(H)|$, and hence $|\mathrm{Orb}(A)|$, is not divisible by 5.

3. Suppose $\mathrm{Orb}(A)$ contains the Sylow 5-subgroup H. Then, as before,

   $$\mathrm{Orb}(A) = \mathrm{Orb}(H) = \{gH : \ g \in G\}.$$

   Thus the orbit of A consists of all left cosets of H. Only one of these cosets is a subgroup, namely H itself, because only H contains the identity e.

We have shown that there is exactly one Sylow 5-subgroup in each of the orbits whose size is not divisible by 5, and no Sylow 5-subgroup in any orbit whose size is divisible by 5. Furthermore, all the Sylow 5-subgroups are accounted for in this way since, for any Sylow 5-subgroup H, we have $H \in X$ and $H \in \mathrm{Orb}(H)$.

We can now use the partition equation for the action to say more about the number of Sylow 5-subgroups.

Suppose that G has m distinct subgroups of order 5, which we call

$$H_1, \ldots, H_m.$$

Each of these belongs to a distinct orbit and so we can write the partition equation as

$$\begin{aligned} |X| &= 3003 \\ &= |\mathrm{Orb}(H_1)| + \cdots + |\mathrm{Orb}(H_m)| + |\mathrm{Orb}(A_{m+1})| + \cdots + |\mathrm{Orb}(A_s)|, \end{aligned}$$

where the sizes of the first m orbits are not divisible by 5 and the sizes of the remaining orbits are.

By the Orbit–Stabiliser Theorem,

$$|G| = 15 = |\mathrm{Orb}(H_i)| \times |\mathrm{Stab}(H_i)|, \quad i = 1, \ldots, m.$$

We showed above that

$$\mathrm{Stab}(H_i) = H_i, \quad i = 1, \ldots, m$$

and so

$$|\mathrm{Stab}(H_1)| = \cdots = |\mathrm{Stab}(H_m)| = 5.$$

Hence

$$|\mathrm{Orb}(H_1)| = \cdots = |\mathrm{Orb}(H_m)| = 3.$$

The sizes of the remaining orbits are divisible by 5, so we have

$$|X| = 3003 = 3m + (\text{a multiple of } 5).$$

Reducing this equation modulo 5 gives

$$3 \equiv 3m \pmod 5.$$

Multiplying both sides by 2, and observing that $2 \times 3 = 6$ is congruent to 1 modulo 5, gives

$$m \equiv 1 \pmod 5.$$

Thus, in any group of order 15, the number of Sylow 5-subgroups is congruent to 1 modulo 5.

In Subsection 1.2 we will show that the argument above generalises to give the following theorem.

Theorem 1.6 *Sylow's Second Theorem*

Let G be a finite group of order n and let p be a prime dividing n. Then the number of distinct Sylow p-subgroups of G is congruent to 1 modulo p.

We ask you to take Sylow's Second Theorem on trust for now. To give an example of its use, the next exercise asks you to apply it to classify all groups of order 15.

Exercise 1.4

Let G be a group of order 15.

(a) Show that two distinct Sylow 5-subgroups of G must have trivial intersection.

(b) Assume that G has m Sylow 5-subgroups and that Sylow's Second Theorem holds, that is, that m is congruent to 1 modulo 5. By counting elements of order 5, show that G has exactly one subgroup of order 5 and hence only four elements of order 5.

(c) Let l be the number of Sylow 3-subgroups of G. Determine, in terms of l, the number of elements of G of order 3.

(d) Assume that Sylow's Second Theorem holds, that is, that l is congruent to 1 modulo 3. By counting the number of elements of G of orders 1, 3 and 5, show (by contradiction) that G has an element of order 15 and, hence, that G is cyclic.

So Sylow's First and Second Theorems have enabled us to show that the only group of order 15 is $\mathbb{Z}_{15}$ (since, as we saw in Chapter 6, all cyclic groups of order n are isomorphic to $\mathbb{Z}_n$). You now know all about the groups of order up to and including 15.

1.2 Sylow's First and Second Theorems

Our main aim in this subsection is to give formal proofs of Sylow's First and Second Theorems. For reference, we restate the first theorem and the related definitions.

Definition 1.7 *Sylow p-subgroup*

Let G be a finite group of order n and let p be a prime dividing n. Let p^α be the highest power of p dividing n. Then a subgroup of G of order p^α is called a **Sylow p-subgroup** of G.

Sylow's First Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then G has a Sylow p-subgroup.

As we indicated in Subsection 1.1, our proof of Sylow's First Theorem will use the action of G defined by left multiplication on the set X of all p^α-element subsets of G.

In Subsection 1.1, we noted that a crucial step in the argument was to show that the size of X is not divisible by p. Since the size of X is given by the number of ways of choosing p^α elements from n elements, we have

$$|X| = {}^nC_{p^\alpha}.$$

We therefore need to consider which powers of p can divide this binomial coefficient.

Example 1.3 from Subsection 1.1 and the discussion following Exercise 1.3 give some clues as to how a general proof can be constructed. In Example 1.3 we had a group of order 20 and considered the set X of all four-element subsets of the group. The calculation of the binomial coefficient is, in detail,

$$\begin{aligned} |X| &= {}^{20}C_4 \\ &= \frac{20 \times (20-1) \times (20-2) \times (20-3)}{4 \times (4-1) \times (4-2) \times (4-3)} \\ &= \frac{5 \times (20-1) \times (10-1) \times (20-3)}{1 \times (4-1) \times (2-1) \times (4-3)}. \end{aligned}$$

The important observation for our current purposes is that any power of 2 that divides a term in the numerator also divides the corresponding term in the denominator, and conversely.

This example suggests that we should write the general formula for the binomial coefficient that we require in the form

$$
\begin{aligned}
{}^{n}C_{p^\alpha} &= \frac{n \times (n-1) \times \cdots \times (n-(p^\alpha-1))}{p^\alpha \times (p^\alpha-1) \times \cdots \times 1} \\
&= \frac{(n-0) \times (n-1) \times \cdots \times (n-(p^\alpha-1))}{(p^\alpha-0) \times (p^\alpha-1) \times \cdots \times (p^\alpha-(p^\alpha-1))}.
\end{aligned}
$$

Given the conditions of Sylow's First Theorem, we can write

$$n = p^\alpha z,$$

where z is not divisible by p. The expression for the binomial coefficient becomes

$${}^{p^\alpha z}C_{p^\alpha} = \frac{(p^\alpha z-0) \times (p^\alpha z-1) \times \cdots \times (p^\alpha z-(p^\alpha-1))}{(p^\alpha-0) \times (p^\alpha-1) \times \cdots \times (p^\alpha-(p^\alpha-1))}.$$

Each term in the numerator is of the form

$$p^\alpha z - k,$$

where $k = 0, \ldots, p^\alpha - 1$. The corresponding terms in the denominator are of the form

$$p^\alpha - k,$$

where $k = 0, \ldots, p^\alpha - 1$.

The case of ${}^{20}C_4$ considered above suggests that the highest powers of p dividing $p^\alpha z - k$ and $p^\alpha - k$ are the same, for each value of k from 0 to $p^\alpha - 1$ (and are in fact the highest power of p dividing k). You will establish this result in the next exercise, which uses the notation described above.

Exercise 1.5

(a) Let k be an integer such that $0 < k < p^\alpha$.

(i) Show that if p^β divides $p^\alpha z - k$, then $\beta < \alpha$.

(ii) Hence show that p^β divides $p^\alpha z - k$ if, and only if, p^β divides k.

(b) Deduce that if p does not divide z, then

$${}^{p^\alpha z}C_{p^\alpha}$$

is not divisible by p.

As we indicated in Subsection 1.1, the fact that if p is a prime that does not divide z then ${}^{p^\alpha z}C_{p^\alpha}$ is not divisible by p is the key to providing a general proof of Sylow's First Theorem.

The special cases dealt with in Subsection 1.1 can now be translated directly into a general proof.

Proof of Sylow's First Theorem Let X be the set of all subsets of G having p^α elements, and let G act on X by left multiplication. Suppose that the distinct orbits under this action are

You have shown in Exercise 1.2 that this *is* a group action.

$$\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s).$$

By the partition equation we know that

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|.$$

The use of group actions to prove Sylow's First Theorem is due to H. Wielandt (in 1959), although the result itself has been established for over a century.

By Exercise 1.5, the left-hand side is not divisible by p. Hence at least one term on the right-hand side is not divisible by p.

Let A be an element of X such that $|\mathrm{Orb}(A)|$ is not divisible by p. The Orbit–Stabiliser Theorem gives

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

But $|G|$ is divisible by p^α and $|\mathrm{Orb}(A)|$ is not divisible by p. It follows that $|\mathrm{Stab}(A)|$ is divisible by p^α. Thus $|\mathrm{Stab}(A)| \geq p^\alpha$.

Now consider any element g of $\mathrm{Stab}(A)$ and fix an element a of A. Since $\mathrm{Stab}(A)$ is the stabiliser of A,

$$ga \in g \wedge A = A.$$

Thus, $ga \in A$ for every element $g \in \mathrm{Stab}(A)$. This implies that

This particular part of the proof does *not* use the fact that $|\mathrm{Orb}(A)|$ is not divisible by p.

$$\mathrm{Stab}(A)a \subseteq A.$$

Hence $|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = p^\alpha$.

It follows that $|\mathrm{Stab}(A)| = p^\alpha$. Thus $\mathrm{Stab}(A)$ is a subgroup of G with order p^α, completing the proof. ■

The action of G on the set X of p^α-element subsets of G provides rather more information than is actually used in the proof of Sylow's First Theorem.

In the proof, the existence of a Sylow p-subgroup was established by showing that the stabiliser of some element $A \in X$ had the correct order. The proof shows that the stabiliser of any $A \in X$, such that $|\mathrm{Orb}(A)|$ is not divisible by p, is a Sylow p-subgroup of G. We will show later that all Sylow p-subgroups arise in this way.

Some parts of the proof did not depend on $|\mathrm{Orb}(A)|$ not being divisible by p. In particular, if $a \in A$ and $g \in \mathrm{Stab}(A)$ then

$$ga \in g \wedge A = A,$$

and so all the elements of the right coset $\mathrm{Stab}(A)a$ are contained in A. On the other hand, if a is any element of A, then a is in the right coset $\mathrm{Stab}(A)a$. Thus any $A \in X$ is the union of some right cosets of its stabiliser $\mathrm{Stab}(A)$, those given by elements of A. Since distinct right cosets are disjoint, this means that A consists of a union of disjoint right cosets of $\mathrm{Stab}(A)$. Because all right cosets have the same size as $\mathrm{Stab}(A)$, $|\mathrm{Stab}(A)|$

divides $|A|$ for any A in X. This argument formalises the proof of Lemma 1.4(a).

Now, as A has p^α elements, the group $\mathrm{Stab}(A)$ is a p-group for any element $A \in X$, whether or not $\mathrm{Stab}(A)$ is a Sylow p-subgroup. This formalises the proof of Lemma 1.4(b).

Let us now move on towards proving Sylow's Second Theorem. We begin with a preliminary result.

Lemma 1.8

Let G be a finite group of order $p^\alpha z$, where p is a prime not dividing z. Let X be the set of p^α-element subsets of G. Then, in the action of G on X by left multiplication, the size of every orbit is divisible by z.

Proof Let G act on X by left multiplication. Then, for any $A \in X$, the Orbit–Stabiliser Theorem gives

$$|G| = p^\alpha z = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

By Lemma 1.4(b), we know that $\mathrm{Stab}(A)$ is a p-group. It follows that $|\mathrm{Orb}(A)|$ is divisible by z. ■

This lemma gives useful information about the number of Sylow p-subgroups, and it is used in the proof of Sylow's Second Theorem.

In Example 1.5, we saw that in a group of order 15 the number of Sylow 5-subgroups is congruent to 1 modulo 5. This result generalises to give Sylow's Second Theorem, which we restate and prove.

Sylow's Second Theorem

Let G be a finite group of order n and let p be a prime dividing n. Then the number of distinct Sylow p-subgroups of G is congruent to 1 modulo p.

Proof Our proof uses the same group action and notation as the proof of Sylow's First Theorem.

This strategy generalises a result we obtained in Example 1.5 of Subsection 1.1.

The strategy for the proof is to show that Sylow p-subgroups are exactly the stabilisers of elements whose orbits have size not divisible by p and that each such orbit contains exactly one Sylow p-subgroup. We then use the partition equation

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|$$

to obtain the required result.

We start by showing that if $A \in X$ is such that $|\mathrm{Orb}(A)|$ is not divisible by p, then $\mathrm{Orb}(A)$ contains a Sylow p-subgroup. Under these conditions we know, from our proof of Sylow's First Theorem, that $H = \mathrm{Stab}(A)$ is a Sylow p-subgroup. We also know, by Lemma 1.4, that for a fixed element $a \in A$, $Ha = A$.

Now the orbit of A includes $a^{-1} \wedge A = a^{-1}A = a^{-1}Ha$. But $a^{-1}Ha$ is the conjugate of H by a^{-1}, and so it is a subgroup of G with the same order as H. In other words, $a^{-1}Ha$ is a Sylow p-subgroup contained in $\mathrm{Orb}(A)$. Thus every orbit whose size is not divisible by p contains a Sylow p-subgroup as an element.

Conversely, consider a Sylow p-subgroup H of G. By the definition of X, the subgroup H is an element of X because $|H| = p^\alpha$. We will show that the stabiliser of H is H itself, that is $\mathrm{Stab}(H) = H$, and hence that H is in an orbit, $\mathrm{Orb}(H)$, whose size is not divisible by p.

By the definition of the action, if $g \in G$ then $g \wedge H = gH$, a left coset of H in G. However, we know that $gH = H$ if, and only if, $g \in H$. So $g \wedge H = H$, i.e. $g \in \mathrm{Stab}(H)$ if, and only if, $g \in H$. This shows that $\mathrm{Stab}(H) = H$. The Orbit–Stabiliser Theorem gives

$$\begin{aligned} p^\alpha z &= |G| \\ &= |\mathrm{Orb}(H)| \times |\mathrm{Stab}(H)| \\ &= |\mathrm{Orb}(H)| \times |H| \\ &= |\mathrm{Orb}(H)| \times p^\alpha. \end{aligned}$$

Hence $|\mathrm{Orb}(H)| = z$ and is not divisible by p, and of course $H \in \mathrm{Orb}(H)$.

We now know that an orbit contains a Sylow p-subgroup if, and only if, the size of the orbit is not divisible by p. The last main step is to show that an orbit can contain at most one Sylow p-subgroup.

Let H be a Sylow p-subgroup. Then $\mathrm{Orb}(H)$ consists of all $g \wedge H = gH$ for $g \in G$, that is, all left cosets of H. However, the only left coset of the subgroup H that is a subgroup of G is H itself. Hence no orbit can contain more than one Sylow p-subgroup.

Thus we have established that each orbit whose size is not divisible by p contains exactly one Sylow p-subgroup and that the orbits whose size is divisible by p contain no Sylow p-subgroups. Hence the number of Sylow p-subgroups is the number of orbits whose size is not divisible by p.

We now separate the terms on the right-hand side of the partition equation

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|$$

into those that are divisible by p and those that are not.

Suppose that G has m distinct Sylow p-subgroups, so the action has m distinct orbits whose size is not divisible by p. We write the partition equation as

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_m)| + |\mathrm{Orb}(A_{m+1})| + \cdots + |\mathrm{Orb}(A_s)|,$$

where the first m terms on the right are not divisible by p and the remaining terms are.

For each of the first m terms, $\mathrm{Stab}(A_i)$ is a Sylow p-subgroup and the Orbit–Stabiliser Theorem gives

$$|G| = p^\alpha z = |\mathrm{Orb}(A_i)| \times |\mathrm{Stab}(A_i)| = |\mathrm{Orb}(A_i)| \times p^\alpha, \quad i = 1, \ldots, m.$$

Thus

$$|\mathrm{Orb}(A_i)| = z, \quad i = 1, \ldots, m.$$

By Lemma 1.8, *all* the terms in the partition equation are divisible by z. As we have seen, the first m terms are z. The remaining terms are divisible both by z and by p and, because p and z are coprime, are divisible by pz. Hence

$$|X| = mz + (\text{terms divisible by } pz),$$

which we can write as $|X| = mz + kpz$ for some integer k.

Before continuing, let us paraphrase the result that we have just obtained. Let G be any group of order $n = p^\alpha z$, where p is a prime that does not divide z. Let m be the number of Sylow p-subgroups of G. Then there exists an integer k (which depends on the specific group G) such that

$$|X| = {}^nC_{p^\alpha} = mz + kpz.$$

We now apply this result to the special case of the cyclic group $\mathbb{Z}_n$ of order n. In this case we know that there is exactly one subgroup belonging to each divisor of n. In particular, there is exactly one subgroup of order p^α, and so $m = 1$ for $\mathbb{Z}_n$. Hence, there exists an integer k' such that ${}^nC_{p^\alpha} = z + k'pz$. We now have two expressions for the binomial coefficient, which we equate:

$$mz + kpz = z + k'pz.$$

Dividing through by z gives $m + kp = 1 + k'p$. Hence, $m - 1 = k'p - kp = p(k' - k)$. So p divides $m - 1$ and $m \equiv 1 \pmod{p}$. This completes the proof. ■

Sylow's Second Theorem places sufficient restriction on the number of distinct Sylow p-subgroups for us to be able to make deductions about groups of some specific orders.

Exercise 1.6

Let G be a group of order 91.

(a) Show that G has only one Sylow 13-subgroup.

(b) By investigating the number of elements of order 7, show that G is cyclic.

Hint: in part (b), argue by contradiction.

We have discussed two examples of groups of order pq, where p and q are distinct primes, namely 15 and 91. On the basis of these examples, it would be tempting to believe that all such groups are cyclic. The existence of the dihedral group D_3 of order $6 = 2 \times 3$ is enough to dispel this belief. However, it is possible to make, and prove, a modified version of this conjecture. The next exercise provides a first step in this direction.

Exercise 1.7

(a) Let G be a group of order pq, where p and q are primes with $p < q$. Show that G has exactly one Sylow q-subgroup.

(b) By considering the order of the conjugates of the Sylow q-subgroup of G, show that it is normal in G.

Exercise 1.7 provides a complete generalisation of part of what we discovered about our earlier examples. For groups of this type, the Sylow q-subgroup (the one of larger prime order) is unique and hence normal.

It is worth observing that the proof of the normality of the Sylow q-subgroup in Exercise 1.7 did not use the fact that we were dealing with a Sylow subgroup, but only that there was a unique subgroup of that order. The solution therefore contains a proof of the following lemma.

Lemma 1.9

If G is a group that has only one subgroup of a particular order, then this subgroup is normal.

So far we have established two of the three results that are collectively known as the Sylow Theorems. The final result also concerns the number of Sylow p-subgroups. We have already shown that this number is congruent to 1 modulo p. It must also be a divisor of the order of the group, although establishing this requires a different group action from the proofs above. We deal with this matter in Subsection 1.3.

Finally, as we observed in Corollary 1.2, the Sylow p-subgroups are p-groups and therefore they contain subgroups corresponding to each divisor of their order. Thus, if G has a Sylow p-subgroup of order p^α, then G also has subgroups of orders

$$p, p^2, \ldots, p^{\alpha-1}.$$

We will consider the number of such subgroups, and provide an alternative proof of their existence, in Section 3.

1.3 Sylow's Third Theorem

In the process of classifying groups of a particular order, knowledge of subgroups is sometimes helpful. The Sylow Theorems provide information about subgroups, based only on the order of the group. In particular, as we have seen in some examples, for certain orders the groups must possess a *normal* Sylow p-subgroup. This knowledge can be useful in reducing the number of possibilities to be considered.

We have established two results about a group G of order $n = p^\alpha z$, where p does not divide z. Firstly, G has at least one subgroup of order p^α. Secondly, the number m of such subgroups is congruent to 1 modulo p.

In this subsection we establish that m divides the order of G. This restriction on m is often useful.

In fact, we establish rather more. Since the conjugate of any subgroup is a subgroup of the same order, we already know that the conjugate of a Sylow p-subgroup is another Sylow p-subgroup. We will prove the converse, that is, that any two Sylow p-subgroups are conjugate.

We will use one group action to establish that Sylow p-subgroups are conjugate and another, based on conjugacy, to derive the result that m divides $|G|$.

Exercise 1.8

Let G be a finite group whose order is divisible by p and let H, K be Sylow p-subgroups of G. Let X be the set of left cosets of K, and for $h \in H$ and $gK \in X$ define

$$h \wedge (gK) = (hg)K.$$

Show that this is an action of H on X.

Exercise 1.9

Let G be a finite group of order $p^\alpha z$, where z is not divisible by p. Let H, K be Sylow p-subgroups of G and X be the set of left cosets of K. Consider the group action of H on X described in Exercise 1.8.

(a) What is the order of X?

(b) Use the Orbit–Stabiliser Theorem to show that $|\mathrm{Orb}(gK)| = p^\beta$ for $0 \leq \beta \leq \alpha$, for every $g \in H$.

(c) Use the partition equation to show that there is some $a \in G$ with $|\mathrm{Orb}(aK)| = 1$.

(d) Show that H and K are conjugate.

The next exercise introduces a second group action and asks you to use it to prove a further result on the number of Sylow p-subgroups.

Exercise 1.10

Let G be a finite group of order $p^\alpha z$, where z is not divisible by p. Let

$$H_1, H_2, \ldots, H_m$$

be all the Sylow p-subgroups of G. Let $X = \{H_1, H_2, \ldots, H_m\}$, and for $g \in G$ and $H_i \in X$ define

$$g \wedge H_i = gH_ig^{-1}.$$

(a) Show that $\wedge$ defines an action of G on X.

(b) How many orbits does this action have?

(c) Use the Orbit–Stabiliser Theorem to show that m divides $|G|$.

Hint: for part (b), use Exercise 1.9.

The solutions to Exercises 1.9 and 1.10 provide the proof of Sylow's Third Theorem.

Theorem 1.10 *Sylow's Third Theorem*

Let G be a finite group. Then all the Sylow p-subgroups of G are conjugate, and the number of Sylow p-subgroups divides $|G|$.

There is a corollary to Sylow's Second and Third Theorems that is slightly easier to use for large values of $|G|$.

Corollary 1.11

Let G be a finite group of order $p^\alpha z$, where p is a prime not dividing z. Let m be the number of Sylow p-subgroups of G. Then m divides z.

Proof By Sylow's Second Theorem, we know that m is congruent to 1 modulo p, so p^α and m are coprime. By Sylow's Third Theorem, we know that m divides $|G| = p^\alpha z$. It follows that m divides z. ■

For reference, we present a complete statement of the Sylow Theorems.

Theorem 1.12 *The Sylow Theorems*

Let G be a finite group of order $n = p^\alpha z$, where p is a prime not dividing z. Let m be the number of subgroups of G of order p^α. Then:

- G has a Sylow p-subgroup, that is, $m \geq 1$
- $m \equiv 1 \pmod{p}$, that is, m is of the form $1 + kp$ for some integer k
- all the Sylow p-subgroups of G are conjugate
- m divides $|G|$, that is, m divides z.

The fact that the number of Sylow p-subgroups divides the order of the group provides shorter proofs of some of the results that have already been obtained.

Exercise 1.11

Let G be a group of order 15. Suppose that G has l Sylow 3-subgroups and m Sylow 5-subgroups.

(a) Show that $l = 1$.

(b) Show that $m = 1$.

(c) Show that G is cyclic.

Exercise 1.12

Let G be a group of order 6. Show that G has a unique Sylow 3-subgroup but could have either one or three Sylow 2-subgroups. By considering the groups of order 6, show that both possibilities occur.

2 Applications of the Sylow Theorems

Having proved the Sylow Theorems, we now investigate some applications.

2.1 Finite abelian groups

In Chapter 6 we were able to show that certain finite abelian groups are a direct product of cyclic groups. These are abelian groups whose order is a product of distinct primes and finite abelian p-groups (see Theorems 3.17 and 3.19 respectively). We are now in a position to extend these results to all finite abelian groups.

We start by proving a lemma based on Proposition 1.9 of Chapter 6.

Lemma 2.1

Let G be a finite abelian group with subgroups $H_1, H_2, \ldots, H_s$ such that $s \geq 2$ and

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_s = \{e\}$$

for each i with $1 \leq i \leq s$.

Then $H_1 \times H_2 \times \cdots \times H_s$ is isomorphic to a subgroup of G.

Proof We prove this result by induction on s. When $s = 2$ the result follows directly from Proposition 1.9 of Chapter 6.

Suppose that the result is true for $s = k$; namely, suppose that if G has subgroups $H_1, H_2, \ldots, H_k$ such that

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k = \{e\}$$

for each $i \in \{1, \ldots, k\}$, then $H_1 \times H_2 \times \cdots \times H_k$ is isomorphic to a subgroup of G.

Now suppose that G has subgroups $H_1, H_2, \ldots, H_{k+1}$ such that

$$H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{k+1} = \{e\}$$

for each $i \in \{1, \ldots, k+1\}$. Then for each $i \in \{1, \ldots, k\}$,

$$\{e\} = H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_{k+1} \supseteq H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k,$$

since $e \in H_{k+1}$. Hence $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_k = \{e\}$. Thus we can apply the induction hypothesis to deduce that $H = H_1 \times H_2 \times \cdots \times H_k$ is isomorphic to a subgroup of G.

Since G is abelian and $H_{k+1} \cap H = \{e\}$, we can now apply Proposition 1.9 of Chapter 6 to deduce that $H \times H_{k+1}$ is isomorphic to a subgroup of G.

The required result follows by (repeated applications of) Proposition 1.10 of Chapter 6 and mathematical induction. ■

Theorem 2.2

Let G be a finite abelian group of order $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where $p_1, p_2, \ldots, p_s$ are distinct primes. Then

$$G \cong G_1 \times G_2 \times \cdots \times G_s,$$

where each G_i is an abelian group of order $p_i^{a_i}$ and hence a direct product of cyclic groups.

Proof By Theorem 1.1 (Sylow's First Theorem), we know that for each distinct prime p_i that divides n there is a Sylow p_i-subgroup G_i of order $p_i^{a_i}$.

Now for each i with $1 \leq i \leq s$,

$$G_i \cap G_1 G_2 \cdots G_{i-1} G_{i+1} \cdots G_s = \{e\},$$

since the order of an element in G_i is coprime to the order of any element in $G_1G_2\cdots G_{i-1}G_{i+1}\cdots G_s$.

Thus, since G is abelian, Lemma 2.1 shows that $G_1 \times \cdots \times G_s$ is isomorphic to a subgroup of G. Since $|G|$ is the product of the orders of the Sylow p_i-subgroups, we can conclude that

$$G \cong G_1 \times \cdots \times G_s.$$

By Theorem 3.19 of Chapter 6, each G_i is a direct product of cyclic groups. The result then follows by Proposition 1.10 of Chapter 6. ■

We have now shown that every finite abelian group is (isomorphic to) a direct product of abelian groups of prime power order and hence can be factorised as a direct product of cyclic groups of prime power order. This decomposition into cyclic groups of prime power order is unique up to the order of the factors.

Exercise 2.1

Find the number of non-isomorphic abelian groups of order 72.

2.2 Exercises using the Sylow Theorems

This subsection consists mainly of exercises of three basic types.

Firstly, you are asked to find the number and type of Sylow subgroups of some specific groups. This process is sometimes referred to as 'finding the Sylow structure of a group'. Secondly, you are asked to use the Sylow Theorems to classify groups of a particular order. Thirdly, you are asked to use the Sylow Theorems to show that certain groups are simple; that is, that they contain no non-trivial, proper, normal subgroups.

This third type of activity needs some comment. When investigating the structure of a group G, the knowledge that G has a non-trivial, proper, normal subgroup N can be useful. We can look at the subgroup N and the quotient group G/N and use them to start building a composition series for G as in Subsection 4.2 of Chapter 7. If a group has a unique Sylow p-subgroup for some prime p, then by Lemma 1.9 the subgroup is normal and so, provided the group is not a p-group, the group cannot be simple.

In a p-group G, the unique Sylow p-subgroup is the whole of G, and so is not a proper subgroup.

We begin with the first type of activity by considering the Sylow subgroups of some familiar groups.

Exercise 2.2

For each of the following groups, find the Sylow p-subgroups for each prime dividing the order.

(a) $\mathbb{Z}_6$

(b) $\mathbb{Z}_3 \times \mathbb{Z}_{15}$

(c) S_3

We next look at the Sylow subgroups of some dihedral groups. When thinking about such groups, it is often useful to have in mind both their algebraic and geometric forms.

For example, geometrically D_7 is the group of symmetries of a regular heptagon (7-gon). Its elements are seven rotations about the centre through angles of $0, \frac{2\pi}{7}, \ldots, \frac{12\pi}{7}$ and seven reflections in the axes of symmetry. If we denote the rotation through $\frac{2\pi}{7}$ by a and a selected reflection by b, we obtain the presentation

$$D_7 = \langle a, b \mid a^7 = e,\ b^2 = e,\ ba = a^6 b\,(= a^{-1}b)\rangle.$$

When we do calculations within a dihedral group, sometimes it is easier to work with the presentation, sometimes with the geometry.

In Section 5 of Chapter 5 we mentioned the distinction between the direct and indirect symmetries of a plane figure. This distinction is relevant to our understanding of conjugacy in dihedral groups. Intuitively, for the symmetries of D_7 imagine that the heptagon is red on one side and blue on the other. Rotations preserve colour, reflections (carried out by turning the heptagon over) change the colour.

This observation makes it clear that conjugates of rotations are rotations. For if r is a rotation and g is any element of the group, consider grg^{-1}. Whatever g does to the colour, that is, preserves or changes it, g^{-1} does the same. Thus grg^{-1} must preserve colour and it is, therefore, a rotation.

Exercise 2.3

Consider the dihedral group D_7.

(a) Show that D_7 has a unique Sylow 7-subgroup.

(b) Using the fact that D_7 is not abelian, show that D_7 has exactly seven Sylow 2-subgroups.

(c) Deduce that all reflections are conjugate in D_7.

(d) Working from the presentation described above, show that each non-identity rotation is conjugate to itself and its inverse only.

(e) Write down the class equation for D_7 and hence find the centre of the group.

The class equation for a group appears in Theorem 2.6 of Chapter 7.

The next exercise asks you to use the Sylow Theorems to investigate groups of order 14. This gives an alternative approach to the one taken in Chapter 7.

Exercise 2.4

Show that there are only two groups of order 14, the cyclic group $\mathbb{Z}_{14}$ and the dihedral group D_7.

Hint: use the Sylow Theorems to deduce the existence of an element a of order 7 and an element b of order 2. By considering cosets, show that these two elements generate the group. By considering the conjugate of a by b, deduce the possible relations between a and b.

Many, but not all, of the results that were obtained in the solution to Exercise 2.3 apply to other dihedral groups.

Exercise 2.5

Consider the dihedral group D_{14} of order 28 with presentation

$$D_{14} = \langle a, b |\ a^{14} = e,\ b^2 = e,\ ba = a^{13}b\ (= a^{-1}b)\rangle.$$

(a) Show that D_{14} has a unique Sylow 7-subgroup.

(b) Show that the elements of D_{14} are of orders 1, 2, 7 and 14 only. Show also that there is exactly one rotation of order 2.

(c) Show that the product of two reflections is a rotation. Deduce that each Sylow 2-subgroup contains two distinct reflections and the unique rotation of order 2 (as well as the identity).

(d) Show that the subgroup $\{e, a^7\}$ is normal and that it is contained in every Sylow 2-subgroup of D_{14}.

(e) Show that D_{14} has exactly seven Sylow 2-subgroups.

In Exercise 1.3(c) we worked with a group of order 15. This is an example of a group of order pq, where p and q are distinct primes, that has a unique (normal) Sylow p-subgroup and a unique (normal) Sylow q-subgroup, from which facts we were able to deduce that the group is cyclic.

However, from our point of view, it is not the fact that the group is cyclic that is of particular interest, but rather that the group is, in fact, the internal direct product of its unique Sylow subgroups. To show that this is true in general, we need a special case of the Internal Direct Product Theorem (Theorem 1.5 of Chapter 6), which we restate here as a reminder.

Internal Direct Product Theorem

If H_1 and H_2 are subgroups of a group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if, and only if, all three of the following conditions hold:

(a) $G = H_1 H_2$

(b) $H_1 \cap H_2 = \{e\}$

(c) H_1 and H_2 are normal subgroups of G.

When these three conditions are satisfied, we say that G is the **internal direct product** of H_1 and H_2.

In the case of a *finite* group, we have the following special case.

Theorem 2.3 *Internal direct product for finite groups*

If H_1 and H_2 are subgroups of a finite group G, then

$$\phi : H_1 \times H_2 \to G$$
$$\phi : (h_1, h_2) \mapsto h_1 h_2$$

is an isomorphism if all three of the following conditions hold:

(a) $|G| = |H_1| \times |H_2|$

(b) $|H_1|$ and $|H_2|$ are coprime

(c) H_1 and H_2 are normal subgroups of G.

Proof We are given that condition (c) of the Internal Direct Product Theorem holds, so we only need to show that $H_1 \cap H_2 = \{e\}$ and that $G = H_1 H_2$.

We know that $H_1 \cap H_2$ is a subgroup of both H_1 and H_2 by Proposition 2.6 of Chapter 5. Then $|H_1 \cap H_2|$ divides both $|H_1|$ and $|H_2|$ by Lagrange's Theorem. Since $|H_1|$ and $|H_2|$ are coprime,

$$|H_1 \cap H_2| = 1$$

and so the intersection is trivial, that is, $H_1 \cap H_2 = \{e\}$.

We can now apply Proposition 1.9 of Chapter 6 to conclude that $|H_1 H_2| = |H_1| \times |H_2|$. By condition (a), this implies that $|G| = |H_1 H_2|$, and hence that $G = H_1 H_2$.

All the conditions of the Internal Direct Product Theorem are satisfied and so $G \cong H_1 \times H_2$, as required. ■

We make two observations about this theorem and proof.

Firstly, the proof can be extended to cover more than two normal subgroups with orders coprime in pairs, the product of whose orders is the order of the group. Formally, this extension requires the Principle of Mathematical Induction. Care is needed when checking the second condition of Corollary 1.7 of Chapter 6.

Secondly, we will often apply Theorem 2.3 when the subgroups are unique Sylow subgroups for various primes. In this case the coprimeness of the orders is guaranteed, as is the product property, and normality is a consequence of the uniqueness.

The group of order 15 that we have already looked at in various ways is of this type. We know that it has a unique Sylow 3-subgroup and a unique Sylow 5-subgroup, both of which are cyclic and which have coprime orders. The group is, therefore, the internal direct product of these subgroups. The cyclicity of the group follows from what we know about the direct product of cyclic groups of coprime orders.

Exercise 2.6

(a) Let G be a group of order 221. Show that G is cyclic.

(b) Why does the argument used in the case $|G| = 221$ fail for a group of order 111?

Finally, you are asked to show that groups of particular orders cannot be simple.

Exercise 2.7

Let G be a group of order 110. Show that G has a non-trivial, proper, normal subgroup.

Exercise 2.8

Show that a group of order 132 cannot be simple.

Hint: consider the possibility that none of the Sylow subgroups is unique and show that this leads to a contradiction.

3 Subgroups of prime power order

The Sylow Theorems deal with the existence and number of Sylow p-subgroups for any prime p dividing the order of the group. Thus if G is a group with

$$|G| = p^\alpha z,$$

where p is prime and z is not divisible by p, then the theorems only give information about the subgroups of order p^α, and not about those of order p^β where $\beta < \alpha$.

As we observed earlier, in Subsection 1.1, because any Sylow p-subgroup H of a group G is a p-group, Theorem 4.3 of Chapter 7 shows that H has subgroups of each power of p from p^0 to p^α. This argument shows that G has subgroups corresponding to every power of p dividing $|G|$.

What is not obvious from this argument is that not only is the number of Sylow p-subgroups congruent to 1 modulo p, but the number of subgroups belonging to a particular integer power p^β of p, where $0 \leq \beta \leq \alpha$, is also congruent to 1 modulo p.

The proofs used for the first two of the Sylow Theorems can be adapted to deal with powers less than the highest. Such adaptation will give a second proof of the existence of such subgroups and also prove the 'congruent to 1 modulo p' result.

What cannot be generalised, because it is not true in general, is the conjugacy property of Sylow p-subgroups. Indeed, a group may have subgroups of the same prime power order that are not even isomorphic, so certainly cannot be conjugate. This is because conjugate subgroups are always isomorphic: by Proposition 2.1 of Chapter 7,

$$x \mapsto gxg^{-1}, \quad g, x \in G$$

defines an isomorphism from G to G that maps a subgroup H to its conjugate subgroup gHg^{-1}.

The next exercise provides an example of a group with non-isomorphic p-subgroups of the same order.

Exercise 3.1

Let D_4 be the dihedral group of order 8 with presentation

$$D_4 = \langle a, b \mid a^4 = e,\ b^2 = e,\ ba = a^{-1}b\ (= a^3b)\rangle.$$

(a) Show that D_4 has a cyclic subgroup of order 4.

(b) Show that $\{e, a^2, b, a^2b\}$ is a subgroup of order 4 isomorphic to the Klein group.

The solution to the previous exercise shows that D_4 has two non-isomorphic 2-subgroups of order 4. Thus the subgroups of D_4 with order 4 cannot all be conjugate.

Along with conjugacy, we also have to discard the result that the number of subgroups belonging to a particular prime power is a divisor of the order of the group. As our proof of the divisibility property used conjugacy, it is not entirely surprising that divisibility is lost too. You might wish to verify that D_4 has three subgroups of order 4, one cyclic and two isomorphic to the Klein group, and of course 3 does not divide $8 = |D_4|$.

Our aim, then, is to prove the following theorem.

Theorem 3.1 *Prime Power Subgroups Theorem*

Let G be a finite group and p be a prime.

If p^β divides $|G|$ then G has a subgroup of order p^β.

If m is the number of distinct subgroups of G of order p^β, then

$$m \equiv 1 \pmod{p}.$$

Our strategy for proving Theorem 3.1 is to examine the steps of the proofs of the first two Sylow Theorems and to generalise them.

The core of the original proofs was a group action on the set of p^α-element subsets of the group. For the generalisation, we define the set X on which G acts by left multiplication to be the set of all p^β-element subsets of G.

As in the first two Sylow Theorems, our proof will start by considering the size of X. We have

$$|X| = {}^nC_{p^\beta}.$$

Unlike in the proofs of the first two Sylow Theorems, this binomial coefficient may well be divisible by p, as the next exercise illustrates.

Exercise 3.2

Let G be a group of order 24 and let X be the set of four-element subsets of G.

(a) Calculate $|X|$.

(b) What is the highest power of 2 that divides $|X|$?

Let Y be the set of two-element subsets of G.

(c) Calculate $|Y|$.

(d) What is the highest power of 2 that divides $|Y|$?

Exercise 3.2 gives a hint as to the general result. For the 2^2-element subsets, 2^1 was the highest power dividing $|X|$. For the 2^1-element subsets, the highest power dividing $|Y|$ was 2^2. In each case, the combination of the size of the subsets and the size of the collection of subsets gave us 2^3 altogether, accounting for all the factors of 2 in the order of G.

Thus, if we are considering the set X of p^β-element subsets, we might expect the highest power of p that divides

$$|X| = {}^nC_{p^\beta}$$

to be $p^{\alpha-\beta}$. Once we establish this fact, the rest of the proof of Theorem 3.1 will follow those of the first two Sylow Theorems exactly.

Proof of Theorem 3.1 Suppose that $|G| = p^\alpha z$, where p does not divide z, and let $0 \leq \beta \leq \alpha$.

Let X be the set of p^β-element subsets of G and let G act on X by left multiplication. Now

This is a group action; the previous proof carries over without change.

$$\begin{aligned} |X| = {}^{p^\alpha z}C_{p^\beta} &= \frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\beta - 1))}{(p^\beta - 0) \times (p^\beta - 1) \times \cdots \times 1} \\ &= \frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\beta - 1))}{(p^\beta - 0) \times (p^\beta - 1) \times \cdots \times (p^\beta - (p^\beta - 1))}. \end{aligned}$$

Each term in the numerator is of the form

$$p^\alpha z - k,$$

where k runs from 0 to $p^\beta - 1$. Equally, each corresponding term in the denominator is of the form

$$p^\beta - k,$$

where k runs from 0 to $p^\beta - 1$.

For all terms except the first, in either numerator or denominator, a term will be divisible by a given power of p if, and only if, k is divisible by that power of p, by the solution to Exercise 1.5. In each such case, the highest power of p dividing corresponding terms in the numerator and denominator will be precisely the same, namely the highest power that divides k.

Once we have cancelled all these powers of p, the only remaining power of p in ${}^{p^\alpha z}C_{p^\beta}$ arises from the first terms, p^α in the numerator and p^β in the denominator. Hence the power of p dividing $|X|$ is

$$\frac{p^\alpha}{p^\beta} = p^{\alpha-\beta}$$

as claimed. Thus, we may write $|X| = p^{\alpha-\beta}y$, where y is not divisible by p.

Now, as with the first two Sylow Theorems, we consider the partition equation for the action of G on X defined by left multiplication.

Suppose that the distinct orbits are $\mathrm{Orb}(A_1), \ldots, \mathrm{Orb}(A_s)$. Then the partition equation gives

$$|X| = |\mathrm{Orb}(A_1)| + \cdots + |\mathrm{Orb}(A_s)|.$$

There must be a term on the right-hand side divisible by a power of p that is at most $p^{\alpha-\beta}$, because, if not, all would be divisible by a higher power, contradicting what we have just proved about $|X|$.

Let A be an orbit whose size is divisible by at most $p^{\alpha-\beta}$. By the Orbit–Stabiliser Theorem, we have

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Consider the powers of p on both sides. On the left we have p^α. The first term on the right contributes *at most* $p^{\alpha-\beta}$. It follows that $|\mathrm{Stab}(A)|$ must contribute at least p^β. Hence

$$|\mathrm{Stab}(A)| \geq p^\beta.$$

As before, we now look at the connection between $\mathrm{Stab}(A)$ and A.

By Lemma 1.4 of this chapter, $|\mathrm{Stab}(A)|$ divides $|A|$. Hence $|\mathrm{Stab}(A)| \leq |A| = p^\beta$.

This second inequality completes the proof that $|\mathrm{Stab}(A)| = p^\beta$ and we have produced the subgroup $\mathrm{Stab}(A)$ of order p^β whose existence was claimed.

We have proved a little more along the way. We started by assuming that $|\mathrm{Orb}(A)|$ was divisible by *at most* $p^{\alpha-\beta}$. We then showed that $|\mathrm{Stab}(A)|$ was precisely p^β. The relation

$$|G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|$$

now shows that $|\mathrm{Orb}(A)|$ is divisible by precisely $p^{\alpha-\beta}$. In fact, we have

$$|\mathrm{Orb}(A)| = p^{\alpha-\beta}z.$$

Also by Lemma 1.4, we know that $\mathrm{Stab}(A_i)$ is a p-group of order p^γ, where $0 \leq \gamma \leq \alpha$, for any $A_i \in X$. Therefore, by the Orbit–Stabiliser Theorem, $|\mathrm{Orb}(A_i)| = p^{\alpha-\gamma}z$, and so the sizes of all orbits are divisible by z. Furthermore,

$$|\mathrm{Stab}(A_i)| \text{ divides } |A_i|,$$

so $\gamma \leq \beta$, and hence $p^{\alpha-\gamma} \geq p^{\alpha-\beta}$.

As in the Sylow proof, the orbits consist of cosets, only one of which can be a subgroup.

Now assume that there are m subgroups of order p^β. As in the proof of Sylow's Second Theorem, each orbit whose size is divisible by precisely $p^{\alpha-\beta}$ contains exactly one subgroup of order p^β. Let these orbits be $\mathrm{Orb}(A_1)$ up to $\mathrm{Orb}(A_m)$. The remaining orbits have sizes divisible by z and a power of p greater than $p^{\alpha-\beta}$, and hence are divisible by $p^{\alpha-\beta+1}z$.

Gathering terms in the partition equation gives

$$|X| = p^{\alpha-\beta}y = mp^{\alpha-\beta}z + (\text{terms divisible by } p^{\alpha-\beta+1}z).$$

Dividing by $p^{\alpha-\beta}$ gives

$$y = mz + kpz$$

for some positive integer k that depends on the particular group of order $p^\alpha z$.

We now do the same as in the proof of Sylow's Second Theorem and apply this result to the cyclic group $\mathbb{Z}_{p^\alpha z}$, of order $p^\alpha z$, for which we know that the corresponding value of m is 1. That is, $y = 1 \times z + k'pz$, for some (other) positive integer k'.

A cyclic group has a unique subgroup corresponding to each divisor of its order.

Equating the two expressions for y gives

$$mz + kpz = z + k'pz.$$

Dividing by z gives

$$m + kp = 1 + k'p.$$

Lastly, reducing modulo p gives

$$m \equiv 1 \,(\text{mod } p).$$

This completes the proof. ■

Theorem 3.1 provides additional restrictions on the number of subgroups of a particular order that a group may possess. These restrictions may be useful when classifying groups of a particular order.

Although we cannot say that two subgroups of a particular prime power order must be conjugate, we can rescue part of Sylow's Third Theorem. Any conjugate of a subgroup of order p^β is also a subgroup of order p^β. If we can show that such a subgroup is unique ($m = 1$), then we can deduce that it is equal to all its conjugates, hence that is normal. However, in the absence of coprimeness, uniqueness is usually hard to prove.

Exercise 3.3

Show that any group of order 196 has a normal subgroup of order 49. Give an example of a group of order 196 that has more than one subgroup of order 7.

This concludes our investigation of subgroups of prime power orders.

4 Groups of order $2p^2$

In this last section of Book B, you will work through a series of exercises that lead to the classification of groups of order $2p^2$, where p is an odd prime. Part of the purpose of this is to pull together various results from the book. Many of the exercises are about applying results that have already been proved, so we suggest that you approach each exercise by first checking for relevant results that might help.

We start with a useful result about direct products.

Exercise 4.1

Let G be a finite group with two subgroups H and K satisfying the following:

1. $H \cap K = \{e\}$
2. $|H||K| = |G|$
3. K is contained in the centre of G.

Show that $G = H \times K$.

Exercise 4.2

Let G and H be finite groups with $|G| = |H|$ and let $\phi : G \to H$ be a homomorphism from G to H. Show that if ϕ is one–one then ϕ is an isomorphism.

An isomorphism from a group to itself is known as an **automorphism**. The next exercise investigates certain automorphisms of cyclic groups of order p^2, where p is an odd prime.

Exercise 4.3

Let $H \cong \mathbb{Z}_{p^2}$, where p is an odd prime number, and let $\phi : H \to H$ be an automorphism of H such that ϕ^2 is the identity.

Show that either ϕ is the identity, or

$$\phi(h) = h^{-1} \quad \text{for all } h \in H.$$

Hint: consider the effect of ϕ on a generator of H.

Exercise 4.4

Let G be a group of order $2p^2$, where p is an odd prime. Let H be a Sylow p-subgroup of G.

(a) Show that H is normal in G. To how many different (up to isomorphism) groups might H be isomorphic? Describe each of these groups.

(b) Let $x \in G$ with $x \notin H$. By considering the natural homomorphism $\theta : G \to G/H$, show that x cannot have order p.

(c) Explain why G has an element a of order 2. Show that the map $\phi : H \to G$ defined by

$$\phi : h \mapsto aha$$

is an automorphism of H.

(d) Show that $G = \{ah : h \in H\} \cup H$. For $h_1, h_2 \in H$, write ah_1ah_2 as an expression involving h_1, h_2 and the automorphism ϕ from part (c).

(e) Show that if $H \cong \mathbb{Z}_{p^2}$ then either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ or $G \cong D_{p^2}$.

(f) Show that G has either $1, p$ or p^2 elements of order 2.

(g) If G has exactly one element of order 2, show that G is abelian and list the possible groups to which G can be isomorphic.

(h) Show that if G has p elements of order 2, then $G \cong D_p \times \mathbb{Z}_p$.

(i) Show that if $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and G has p^2 elements of order 2, then G is uniquely determined up to isomorphism.

The solution to Exercise 4.4 shows that a group of order $2p^2$ is isomorphic to one of:

- $\mathbb{Z}_{2p^2}$
- $\mathbb{Z}_{2p} \times \mathbb{Z}_p$
- $D_p \times \mathbb{Z}_p$
- the group described in part (i) of the exercise.

In other words, we have obtained a classification for the groups of order $2p^2$, where p is an odd prime. The group described in part (i) is an example of a structure known as a *semidirect product*. In the case $p = 3$, so that we are considering groups of order 18, this structure is the subgroup of S_6 generated by $(1\,2\,3), (4\,5\,6)$ and $(1\,3)(4\,6)$: the 3-cycles $(1\,2\,3)$ and $(4\,5\,6)$ generate the $\mathbb{Z}_3 \times \mathbb{Z}_3$ subgroup, and $(1\,3)(4\,6)$ is the element a of order 2.

Learning outcomes

We list those topics on which we may set assessment questions to test your understanding of the chapter.

After working through this chapter you should be able to:

(a) Apply the Sylow Theorems to make deductions about the existence of subgroups of certain orders.

(b) Apply the Sylow Theorems to the classification of groups of a particular order (in simple cases).

(c) Apply counting arguments based on group actions to simple cases.

(d) List all possible abelian groups of a given finite order.

(e) Follow the style of proof used in proving the Sylow Theorems.

Solutions to exercises

Solution to Exercise 1.1

Let G be any group of order 20. Let X be the set of all five-element subsets of G and define an action of G on X by

$$g \wedge A = gA$$

for every element A of X.

The number of five-element subsets of G is

$$\begin{aligned} {}^{20}C_5 &= \frac{20 \times 19 \times 18 \times 17 \times 16}{5 \times 4 \times 3 \times 2 \times 1} \\ &= \frac{4 \times 19 \times 6 \times 17 \times 16}{1 \times 4 \times 1 \times 2 \times 1} \\ &= 19 \times 6 \times 17 \times 8 \\ &= 15504. \end{aligned}$$

Thus $|X| = 15504$.

In Example 1.3, the significant fact about $|X|$ was that it was not divisible by the prime being considered (2 in the example). Here, $|X| = 15504$ is not divisible by 5.

Suppose that

$$\mathrm{Orb}(A_1), \mathrm{Orb}(A_2), \ldots, \mathrm{Orb}(A_s)$$

are the distinct orbits for this group action. Then

$$15504 = |\mathrm{Orb}(A_1)| + |\mathrm{Orb}(A_2)| + \cdots + |\mathrm{Orb}(A_s)|.$$

If all the terms on the right-hand side were divisible by 5, then so would be the left-hand side. It follows that at least one term on the right-hand side is not divisible by 5.

Suppose that A is an element of X such that $|\mathrm{Orb}(A)|$ is not divisible by 5. The Orbit–Stabiliser Theorem gives

$$20 = |G| = |\mathrm{Orb}(A)| \times |\mathrm{Stab}(A)|.$$

Since $|\mathrm{Orb}(A)|$ is not divisible by 5, $|\mathrm{Stab}(A)|$ must be. Hence

$$|\mathrm{Stab}(A)| \geq 5.$$

As in the example, we now derive the opposite inequality.

If g is any element of $\mathrm{Stab}(A)$ then

$$g \wedge A = gA = A.$$

Thus, for a fixed element a of A, we have $ga \in A$, for all elements g of $\mathrm{Stab}(A)$. Hence the whole of the right coset

$$\mathrm{Stab}(A)a \subseteq A.$$

Thus, because a right coset has the same number of elements as the subgroup from which it is formed,

$$|\mathrm{Stab}(A)| = |\mathrm{Stab}(A)a| \leq |A| = 5.$$

Hence $|\mathrm{Stab}(A)| = 5$ and $\mathrm{Stab}(A)$ is a subgroup of G of order 5.

Solution to Exercise 1.2

We have to show that if A is a subset of G with k elements, then so is gA. Since gA consists of products of elements of G, by closure it is a subset of G.

We show that gA has k elements by showing that the function from A to gA defined by

$$a \mapsto ga$$

is one–one and onto.

Suppose that $ga_1 = ga_2$. Then, by left cancellation, $a_1 = a_2$. Hence the function is one–one.

Since every element of gA is of the form ga for some element a of A, the function is onto.

Thus A and gA have the same number of elements, k, and so $g \wedge A = gA \in X$. We now check that $\wedge$ satisfies the conditions in the definition of a group action.

(a) We have $e \wedge A = eA = \{ea : a \in A\} = \{a : a \in A\} = A$.

(b) By the definition of $\wedge$ and associativity in G, if g and h are elements of G, we have

$$\begin{aligned}(gh) \wedge A &= (gh)A \\ &= \{(gh)a : a \in A\} \\ &= \{g(ha) : a \in A\} \\ &= g \wedge \{ha : a \in A\} \\ &= g \wedge (hA) \\ &= g \wedge (h \wedge A).\end{aligned}$$

Solution to Exercise 1.3

(a) The highest power of 3 that divides 24 is $3^1 = 3$. Also

$$\begin{aligned}{}^{24}C_3 &= \frac{24 \times 23 \times 22}{3 \times 2 \times 1} \\ &= \frac{8 \times 23 \times 22}{1 \times 2 \times 1} \\ &= 8 \times 23 \times 11 \ (= 2024),\end{aligned}$$

which is not divisible by 3. This fills in the gap in the generalisation of Example 1.3, and we may deduce that any group of order 24 has a subgroup of order 3.

(b) The highest power of 2 dividing 24 is $2^3 = 8$. We have

$$
\begin{aligned}
{}^{24}C_8 &= \frac{24 \times 23 \times 22 \times 21 \times 20 \times 19 \times 18 \times 17}{8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1} \\
&= \frac{3 \times 23 \times 11 \times 21 \times 5 \times 19 \times 9 \times 17}{1 \times 7 \times 3 \times 5 \times 1 \times 3 \times 1 \times 1} \\
&= 23 \times 11 \times 3 \times 19 \times 3 \times 17 \ (= 735471),
\end{aligned}
$$

which is not divisible by 2. As above, we may deduce that every group of order 24 has a subgroup of order 8.

(c) The calculations are slightly shorter here.

$$
\begin{aligned}
{}^{15}C_3 &= \frac{15 \times 14 \times 13}{3 \times 2 \times 1} \\
&= \frac{5 \times 7 \times 13}{1 \times 1 \times 1} \\
&= 5 \times 7 \times 13 \ (= 455),
\end{aligned}
$$

which is not divisible by 3. Hence G has a subgroup H of order 3.

$$
\begin{aligned}
{}^{15}C_5 &= \frac{15 \times 14 \times 13 \times 12 \times 11}{5 \times 4 \times 3 \times 2 \times 1} \\
&= \frac{3 \times 7 \times 13 \times 6 \times 11}{1 \times 2 \times 3 \times 1 \times 1} \\
&= 3 \times 7 \times 13 \times 11 \ (= 3003),
\end{aligned}
$$

which is not divisible by 5. Hence G has a subgroup K of order 5.

Solution to Exercise 1.4

(a) The subgroup that is the intersection of two Sylow 5-subgroups must, by Lagrange's Theorem, have order 1 or 5. Since the subgroups are distinct, the intersection must have order 1 and hence be trivial.

(b) There are m subgroups of order 5, where m is congruent to 1 modulo 5. The possibilities for m are $1, 6, \ldots$. However, by part (a), every new five-element subgroup contributes four more non-identity elements of order 5. Thus, if there were six or more such subgroups, we would have the identity plus at least 24 other elements. Since this is impossible, we conclude that $m = 1$.

This unique Sylow 5-subgroup contains the identity and four elements of order 5. Since any element of order 5 in G would generate a Sylow 5-subgroup, G can have only these four elements of order 5.

(c) By a similar argument to that for order 5 in part (a), any two distinct subgroups of order 3 have trivial intersection. Each such subgroup has two non-identity elements of order 3. Hence there are $2l$ elements of order 3 in G.

(d) Elements of G can only have orders 1, 3, 5 and 15.

The identity is the only element of order 1.

There are four elements of order 5.

There are $2l$ elements of order 3.

If there are no elements of order 15 then we must have

$$15 = 1 + 4 + 2l,$$

which gives $l = 5$. However, 5 is not congruent to 1 modulo 3 as required by Sylow's Second Theorem. This contradiction shows that G must have an element of order 15, and so it is cyclic.

Solution to Exercise 1.5

(a) (i) Suppose that p^β divides $p^\alpha z - k$. Then

$$p^\alpha z - k = p^\beta l$$

for some integer l. Thus

$$k = p^\alpha z - p^\beta l.$$

Suppose now that $\beta \geq \alpha$, so that $p^\beta \geq p^\alpha$. Then

$$\begin{aligned} k &= p^\alpha z - p^\beta l \\ &= p^\alpha (z - p^{\beta-\alpha} l). \end{aligned}$$

Thus p^α divides k, contradicting the fact that $0 < k < p^\alpha$. Hence $\beta < \alpha$ as required.

(ii) Again suppose that p^β divides $p^\alpha z - k$. Then, as above,

$$k = p^\alpha z - p^\beta l$$

for some integer l. By part (i), we have $\beta < \alpha$, so that $p^\alpha > p^\beta$. Therefore

$$\begin{aligned} k &= p^\alpha z - p^\beta l \\ &= p^\beta \big(p^{\alpha-\beta} z - l\big). \end{aligned}$$

Thus p^β divides k.

Conversely, suppose that p^β divides k. Then, as $0 < k < p^\alpha$, we must have $\beta < \alpha$ and so p^β divides p^α. Hence p^β divides both terms in

$$p^\alpha z - k,$$

and therefore divides $p^\alpha z - k$.

(b) Consider the terms in the binomial coefficient

$$\frac{(p^\alpha z - 0) \times (p^\alpha z - 1) \times \cdots \times (p^\alpha z - (p^\alpha - 1))}{(p^\alpha - 0) \times (p^\alpha - 1) \times \cdots \times (p^\alpha - (p^\alpha - 1))}.$$

Since p does not divide z, the power of p dividing the first term in the numerator is the same as the power of p dividing the first term in the denominator, namely p^α.

Each remaining term in the numerator is of the form $p^\alpha z - k$ with $0 < k < p^\alpha$. By part (a), the maximum power of p dividing $p^\alpha z - k$ is the maximum power of p dividing k. This is true for all integer values of z. In particular, it is true for the case $z = 1$. Hence, the maximum power of p dividing k is also the maximum power of p dividing $p^\alpha 1 - k = p^\alpha - k$, which is the term in the denominator corresponding to $p^\alpha z - k$ in the numerator.

Hence each factor of p in the numerator is cancelled out by a corresponding factor of p in the denominator.

Thus the binomial coefficient ${}^{p^\alpha z}C_{p^\alpha}$ is not divisible by p.

Solution to Exercise 1.6

(a) Since $91 = 7 \times 13$, the Sylow 13-subgroups of G are of order 13 and hence cyclic. By an argument used in Exercise 1.4, any two distinct subgroups of order 13 will have trivial intersection. Thus each new subgroup of order 13 contributes twelve additional elements of order 13.

If G has m Sylow 13-subgroups, then m is congruent to 1 modulo 13. Thus the possibilities for m are $m = 1, 14, \ldots$. But 14 such subgroups would contain

$$1 + 14 \times 12 = 169$$

distinct elements, a contradiction since $|G| = 91$. Thus $m = 1$.

(b) So far, we know that G has one element of order 1 and twelve of order 13 (in the unique Sylow 13-subgroup). We now show that the remaining 78 elements cannot all be of order 7.

Since $91 = 7 \times 13$, the Sylow 7-subgroups of G must be cyclic and of order 7. As before, any two distinct such subgroups have trivial intersection. Suppose that G has l Sylow 7-subgroups. Each such subgroup accounts for six elements of G of order 7.

Assume that there are no elements of order 91 (the only remaining possible order). Counting the elements of G gives

$$91 = 1 + 12 + 6l,$$

which requires $l = 13$. But 13 is not congruent to 1 modulo 7, contradicting Sylow's Second Theorem.

Thus G has at least one element of order 91 and so it is cyclic.

Solution to Exercise 1.7

(a) Since $|G| = pq$, the Sylow q-subgroups of G are of prime order q and hence cyclic.

As in the solutions to Exercises 1.4 and 1.6, each such subgroup has $q-1$ elements of order q and any two distinct such subgroups have trivial intersection. So each new subgroup of order q contributes $q-1$ additional elements of order q.

If G has m Sylow q-subgroups, then m is congruent to 1 modulo q and so the possibilities for m are $m = 1, q+1, \ldots$. However, $q+1$ such subgroups would contain

$$1 + (q+1)(q-1) = 1 + q^2 - 1 = q^2$$

elements. Since $p < q$, we have

$$|G| = pq < qq = q^2.$$

This contradiction shows that $m = 1$.

Sylow's Third Theorem, which we discuss in the next subsection, provides a shorter proof that the subgroup is unique.

(b) The conjugate of a subgroup is a subgroup having the same order. Since any Sylow q-subgroup H is unique, all conjugates of H must be H itself. That is,

$$gHg^{-1} = H, \quad \text{for all } g \in G,$$

and so H is normal in G.

Solution to Exercise 1.8

First of all, we see that $h \wedge (gK) = (hg)K \in X$ for all $g \in G$ and all $h \in H$, so that $\wedge$ indeed defines a function from $H \times X$ to X. We check that this function satisfies the properties in Definition 3.1 of Chapter 6.

(a) $e \wedge (gK) = (eg)K = gK$ for all $g \in G$.

(b) If $h_1, h_2 \in H$ then
$h_1 \wedge (h_2 \wedge (gK)) = h_1 \wedge (h_2 gK) = (h_1 h_2 gK) = (h_1 h_2) \wedge gK$.

Solution to Exercise 1.9

(a) Since $|K| = p^\alpha$, Lagrange's Theorem implies that $|X| = z$.

(b) From the Orbit–Stabiliser Theorem,

$$|H| = |\mathrm{Orb}(gK)| \times |\mathrm{Stab}(gK)|.$$

The result $|\mathrm{Orb}(gK)| = p^\beta$ follows from $|H| = p^\alpha$.

(c) Suppose that this action has s distinct orbits. Then the partition equation gives

$$\begin{aligned} z = |X| &= |\mathrm{Orb}(g_1K)| + |\mathrm{Orb}(g_2K)| + \cdots + |\mathrm{Orb}(g_sK)| \\ &= p^{\beta_1} + p^{\beta_2} + \cdots + p^{\beta_s}. \end{aligned}$$

Since z is not divisible by p, there must be at least one $\beta_i = 0$, that is, $|\mathrm{Orb}(g_iK)| = 1$. Then g_i is the required a.

(d) From part (c), we know there is $a \in G$ such that $|\mathrm{Orb}(aK)| = 1$. Then for all $h \in H$ we have $h \wedge (aK) = aK$, that is,

$$(ha)K = aK.$$

This tells us that $a^{-1}(ha)K = K$, so $a^{-1}ha \in K$. Since this holds for all $h \in H$, we have

$$a^{-1}Ha \subseteq K.$$

But $|H| = |K| = p^\alpha$, and $|a^{-1}Ha| = |K|$, therefore $a^{-1}Ha = K$ and so H and K are conjugate, as required.

Solution to Exercise 1.10

(a) Since the conjugate of a Sylow p-subgroup is again a Sylow p-subgroup, we have that

$$g \wedge H_i = gH_ig^{-1}$$

for all $g \in G$ and H_i in X. Therefore $\wedge$ defines a function from $G \times X$ to X. We check that the properties in Definition 3.1 of Chapter 6 hold.

(i) Since $eH_ie^{-1} = eH_ie = H_i$, we have $e \wedge H_i = H_i$ for all $H_i \in X$.

(ii) Let $g_1, g_2 \in G$. Then

$$\begin{aligned} g_1 \wedge (g_2 \wedge H_i) &= g_1 \wedge (g_2H_ig_2^{-1}) \\ &= g_1(g_2H_ig_2^{-1})g_1^{-1} \\ &= (g_1g_2)H_i(g_1g_2)^{-1} \\ &= (g_1g_2) \wedge H_i. \end{aligned}$$

(b) From Exercise 1.9, we know that all Sylow p-subgroups are conjugate. This means there is only one orbit.

(c) Since there is only one orbit, we know $|\mathrm{Orb}(H_1)| = |X| = m$, so the Orbit–Stabiliser Theorem gives

$$|G| = |\mathrm{Orb}(H_1)| \times |\mathrm{Stab}(H_1)| = m \times |\mathrm{Stab}(H_1)|.$$

Solution to Exercise 1.11

(a) We know that l is congruent to 1 modulo 3 and that l divides 5. The first requirement gives $l = 1, 4, 7, \ldots$, and the only one of these values satisfying the second restriction is $l = 1$.

(b) We know that m is congruent to 1 modulo 5 and that m divides 3. The first requirement gives $m = 1, 6, 11, \ldots$, and the only one of these values satisfying the second restriction is $m = 1$.

(c) We now know that G contains the identity, just four elements of order 5 and just two elements of order 3. The remaining eight elements must, therefore, have order 15 (the only remaining possible order). Hence G is cyclic.

Solution to Exercise 1.12

Suppose that G has l Sylow 3-subgroups. Then l is congruent to 1 modulo 3, that is, $l = 1, 4, 7, \ldots$. Among these possible values for l, only 1 divides 2. Hence G has a unique Sylow 3-subgroup.

Suppose that G has m Sylow 2-subgroups. Then m is congruent to 1 modulo 2. So $m = 1, 3, 5, \ldots$, of which both 1 and 3 divide 3. Hence G could have one or three Sylow 2-subgroups.

There are only two different groups of order 6, namely $\mathbb{Z}_6$ and S_3.

Since $\mathbb{Z}_6$ is cyclic, it has a unique subgroup corresponding to each divisor of its order. Thus, $\mathbb{Z}_6$ has one Sylow 2-subgroup.

In S_3, each of the 2-cycles $(1\,2), (1\,3)$ and $(2\,3)$ generates a distinct subgroup of order 2. Hence S_3 has three Sylow 2-subgroups.

Solution to Exercise 2.1

Let G be an abelian group of order 72. Since $72 = 8 \times 9 = 2^3 \times 3^2$, by Theorem 2.2 we have $G \cong H \times K$, where H has order 8 and K has order 9.

The possibilities for H are

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

and the possibilities for K are

$$\mathbb{Z}_9, \quad \mathbb{Z}_3 \times \mathbb{Z}_3.$$

It follows that G is one of

- $\mathbb{Z}_8 \times \mathbb{Z}_9 (\cong \mathbb{Z}_{72})$
- $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_{24} \times \mathbb{Z}_3)$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 (\cong \mathbb{Z}_{36} \times \mathbb{Z}_2 \cong \mathbb{Z}_4 \times \mathbb{Z}_{18})$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_{12} \times \mathbb{Z}_6)$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 (\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18})$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 (\cong \mathbb{Z}_6 \times \mathbb{Z}_6 \times \mathbb{Z}_2)$.

Therefore there are six abelian groups of order 72 up to isomorphism.

Solution to Exercise 2.2

(a) Firstly, since $\mathbb{Z}_6$ is abelian, there is a normal Sylow subgroup for each prime divisor. The conjugacy part of Sylow's Third Theorem, together with normality, tells us that this subgroup is unique.

Since $|\mathbb{Z}_6| = 2 \times 3$, the Sylow 2-subgroup has order 2, hence it is (isomorphic to) $\mathbb{Z}_2$. Similarly, the Sylow 3-subgroup is $\mathbb{Z}_3$.

In terms of the elements of $\mathbb{Z}_6$, the subgroups are

$$\{0, 3\} \quad \text{and} \quad \{0, 2, 4\}.$$

(b) Since the group is abelian, the argument about uniqueness of Sylow p-subgroups given in part (a) holds here too. The group has order

$$3 \times 15 = 3^2 \times 5.$$

Since 3 and 5 are coprime, we know that $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$, so

$$\mathbb{Z}_3 \times \mathbb{Z}_{15} \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_5.$$

Thus the Sylow 3-subgroup (of order 3^2) is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ and the Sylow 5-subgroup (of order 5) is isomorphic to $\mathbb{Z}_5$.

As a subgroup of $\mathbb{Z}_3 \times \mathbb{Z}_{15}$, the Sylow 3-subgroup is

$$\mathbb{Z}_3 \times \{0, 5, 10\}.$$

Similarly, the Sylow 5-subgroup is

$$\{0\} \times \{0, 3, 6, 9, 12\}.$$

(c) The order of S_3 is $6 = 2 \times 3$. Since S_3 is not abelian, we cannot argue as above that the Sylow subgroups are unique.

However, the Sylow 3-subgroup is unique, for the following reasons. If there are m Sylow 3-subgroups, then we know that

$$m \equiv 1 \,(\mathrm{mod}\ 3) \quad \text{and} \quad m \mid 2.$$

The only solution is $m = 1$.

We can also derive this result from knowledge of the elements of S_3. Any Sylow 3-subgroup must be cyclic and of order 3. There are only two elements of order 3, namely the 3-cycles

$$(1\,2\,3) \quad \text{and} \quad (1\,3\,2).$$

Thus the only possibility for a Sylow 3-subgroup is

$$\{e, (1\,2\,3), (1\,3\,2)\}.$$

Since this is a subgroup, it must be the unique Sylow 3-subgroup.

Any Sylow 2-subgroup must be cyclic and of order 2. There are three elements of order 2, the 2-cycles

$$(1\,2), \quad (1\,3) \quad \text{and} \quad (2\,3).$$

Each 2-cycle generates a cyclic subgroup of order 2, so the Sylow 2-subgroups are

$$\{e, (1\,2)\}, \quad \{e, (1\,3)\} \quad \text{and} \quad \{e, (2\,3)\}.$$

The number of Sylow 2-subgroups is 3. As a check,

$$3 \equiv 1 \,(\mathrm{mod}\ 2) \quad \text{and} \quad 3 \mid 6.$$

Note that, as expected from the theory, all the Sylow 2-subgroups are conjugate because their generators have the same cycle type and are, therefore, conjugate in S_3.

Solution to Exercise 2.3

(a) There are several perfectly good proofs that D_7 has a unique Sylow 7-subgroup. All use the fact that, since the order of D_7 is $14 = 2 \times 7$, any Sylow 7-subgroup has order 7.

First proof
Any Sylow 7-subgroup must contain a generator of order 7. The only elements of order 7 are the non-trivial rotations. The rotation subgroup contains all such elements, has order 7 and so it must be the unique Sylow 7-subgroup.

Second proof
Any Sylow 7-subgroup has index 2. Therefore it is normal, and hence unique.

Third proof
The number of Sylow 7-subgroups is congruent to 1 modulo 7. Possible numbers are 1, 8, ... Each such subgroup would contribute six 'new' elements of order 7, so eight or more such subgroups are impossible. Thus the Sylow 7-subgroup is unique.

Fourth proof
The number of Sylow 7-subgroups is congruent to 1 modulo 7 and divides 2. The only possibility is 1.

(b) Any Sylow 2-subgroup of D_7 has order 2 and hence it is cyclic. Again, there are several possible proofs that there are seven such subgroups. We give two.

First proof
There are seven reflections in D_7. Each generates a distinct subgroup of order 2, which is a Sylow 2-subgroup. There are no other elements of order 2.

Second proof
The number of Sylow 2-subgroups is congruent to 1 modulo 2, that is, it is odd, and divides 7. The possibilities are 1 and 7.

Suppose there is a unique Sylow 2-subgroup. We count the elements of various orders. There is only one element of order 1. There are six elements of order 7 in the unique Sylow 7-subgroup. By our assumption, there is only one element of order 2. We have accounted for only eight elements of G. Hence the remaining elements must have order 14 (the only other possible order). This forces

$$D_7 \cong \mathbb{Z}_{14},$$

a contradiction because $\mathbb{Z}_{14}$ is abelian and D_7 is not.

The only remaining possibility is that there are seven Sylow 2-subgroups.

(c) In a Sylow 2-subgroup, each reflection is the non-identity element. As all such subgroups are conjugate and the identity always conjugates to itself, the result follows.

(d) Using the notation of the presentation, the non-identity rotations are

$$a, a^2, a^3, a^4, a^5, a^6.$$

Conjugating a^i by another rotation a^j gives

$$a^j a^i a^{-j} = a^{j+i-j} = a^i.$$

Conjugating by a reflection $a^j b$ gives

$$\begin{aligned}(a^j b)a^i(a^j b)^{-1} &= a^j(ba^i)b^{-1}a^{-j} \\ &= a^j a^{-i} b b^{-1} a^{-j} \qquad (\text{since } ba^i = a^{-i}b) \\ &= a^{j-i-j} \\ &= a^{-i}.\end{aligned}$$

Thus every conjugate of a rotation is either itself or its inverse.

(e) The various calculations above show that the conjugacy classes in D_7 are

$$\{e\},\ \{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\},\ \{a, a^6\},\ \{a^2, a^5\},\ \{a^3, a^4\}.$$

The class equation is

$$14 = 1 + 7 + 2 + 2 + 2.$$

The centre consists of the single-element conjugacy classes. Hence the centre of D_7 is the trivial subgroup $\{e\}$.

Solution to Exercise 2.4

We already know, from our work on abelian groups, that there is only one abelian group of order 14, namely $\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7$.

Let G be any group of order 14.

By the Sylow Theorems, there is a unique (normal) Sylow 7-subgroup, which must be cyclic and of order 7. Let this subgroup be

$$\langle a \mid a^7 = e \rangle.$$

Again by the Sylow Theorems, there is at least one Sylow 2-subgroup – in fact, there are either one or seven Sylow 2-subgroups. Let

$$\langle b \mid b^2 = e \rangle$$

be one such subgroup.

Because b has order 2, it is not an element of $\langle a \rangle$. Therefore the cosets

$$\begin{aligned}\langle a \rangle &= \{e, a, a^2, a^3, a^4, a^5, a^6\} \qquad \text{and} \\ \langle a \rangle b &= \{b, ab, a^2b, a^3b, a^4b, a^5b, a^6b\}\end{aligned}$$

are distinct and give all 14 elements of G. In particular, a and b generate G.

We now have most of the ingredients for a presentation of D_7. All that is left to do is to show that $ba = a^{-1}b$, or equivalently that $bab^{-1} = a^{-1}$.

The element bab^{-1} is a conjugate of a and so, as you can easily check, has order 7 (remember that conjugate elements always have the same order).

It therefore belongs to the unique subgroup of order 7 generated by a. Hence

$$bab^{-1} = a^i \quad \text{for some integer } i \in \{1, 2, \ldots, 6\}.$$

Note that as bab^{-1} has order 7, it cannot be the identity, which excludes $i = 0$.

Conjugating again by b gives

$$\begin{aligned} b^2ab^{-2} &= b(bab^{-1})b^{-1} \\ &= ba^ib^{-1} \\ &= (bab^{-1})^i \\ &= (a^i)^i \\ &= a^{i^2}. \end{aligned}$$

Since $b^2 = e$, this gives $a = a^{i^2}$. So, as a has order 7, $i^2 \equiv 1 \,(\text{mod } 7)$ and, by exhaustion, $i = 1$ or 6.

If $i = 1$ then a and b commute. Since a and b generate G, this implies that G is abelian and hence

$$G \cong \mathbb{Z}_{14}.$$

We are left with the case $i = 6$, that is, $bab^{-1} = a^6 = a^{-1}$. So in this case

$$G \cong \langle a, b \mid a^7 = e,\ b^2 = e,\ ba = a^6b\,(= a^{-1}b)\rangle = D_7.$$

Solution to Exercise 2.5

Since the order of D_{14} is $28 = 2^2 \times 7$, the Sylow subgroups have orders 4 and 7. Any Sylow 7-subgroup must be cyclic. A Sylow 2-subgroup is either cyclic or the Klein group.

(a) The number of Sylow 7-subgroups must be one of 1, 8, ... as well as being a divisor of 4. The only possibility is 1.

(b) The identity e has order 1.

The 14 reflections

$$b, ab, a^2b, \ldots, a^{13}b$$

all have order 2.

The rotations form the subgroup

$$\{e, a, a^2, \ldots, a^{13}\},$$

which is of order 14. Thus, the only possible orders of the non-identity rotations are 2, 7 and 14. From our knowledge of cyclic groups, we know that each of these does occur. For example, a has order 14, a^2 has order 7 and a^7 has order 2.

In fact, the orders of the rotations are as follows.

Order 1: e.
Order 2: a^7.
Order 7: $a^2, a^4, a^6, a^8, a^{10}, a^{12}$.
Order 14: $a, a^3, a^5, a^9, a^{11}, a^{13}$.

So a^7 is the only rotation of order 2.

(c) The most straightforward argument is the direct/indirect symmetry one. Suppose that the 14-gon is coloured red on one side and blue on the other. Since each reflection changes the colour of a 14-gon, the product of two reflections preserves the colour and so is a rotation. Note that this includes the identity rotation, which is produced just in those cases where the two reflections are identical.

Any Sylow 2-subgroup has order 4 and so it can only contain elements of orders 1, 2 and 4. There are no elements of order 4, so each Sylow 2-subgroup contains the identity and three elements of order 2 (so is the Klein group).

There is only one rotation of order 2. Thus at least two elements of a Sylow 2-subgroup are reflections. However, the product of two such *distinct* reflections is a non-identity rotation. Thus each Sylow 2-subgroup contains two distinct reflections and the unique rotation of order 2.

(d) Any conjugate of a^7, the rotation of order 2, must be another rotation of order 2, since conjugation preserves order (Proposition 2.5 of Chapter 5) and maps direct symmetries to direct symmetries. There is only one such rotation, so the subgroup

$$\{e, a^7\}$$

has no conjugate subgroups apart from itself, and hence is normal by Proposition 3.10 of Chapter 5.

Alternatively, the subgroup $\{e, a^7\}$ is a union of conjugacy classes, and hence it is normal by Proposition 3.12 of Chapter 5.

From part (c), $\{e, a^7\}$ lies in every Sylow 2-subgroup.

(e) The number of Sylow 2-subgroups is odd (congruent to 1 modulo 2) and divides 7. Therefore the only possibilities are 1 and 7.

There are several ways to rule out 1, the easiest of which is as follows.

Each Sylow 2-subgroup contains e, a^7 and two 'new' reflections. There are, in all, 14 reflections (of order 2). To account for them requires seven Sylow 2-subgroups.

Solution to Exercise 2.6

(a) We have

$$|G| = 221 = 13 \times 17.$$

The number of Sylow 13-subgroups of G is congruent to 1 modulo 13 and divides 17. Thus there is a unique Sylow 13-subgroup.
The number of Sylow 17-subgroups is congruent to 1 modulo 17 and divides 13. Thus there is a unique Sylow 17-subgroup.

Therefore G has unique, normal, cyclic Sylow subgroups of coprime orders 13 and 17. Hence, by Theorem 2.3 and Theorem 2.11 of Chapter 6,

$$G \cong \mathbb{Z}_{13} \times \mathbb{Z}_{17} \cong \mathbb{Z}_{221},$$

and G is cyclic.

(b) Since $111 = 3 \times 37$, an argument like that in part (a) shows that a group of order 111 must have a unique Sylow 37-subgroup. However, the number of Sylow 3-subgroups can be either 1 or 37, since both are congruent to 1 modulo 3 and both divide 37. We therefore cannot be sure that there is a unique Sylow 3-subgroup.

Solution to Exercise 2.7

The order of G has prime decomposition

$$110 = 2 \times 5 \times 11.$$

We check the number of Sylow subgroups corresponding to 2, 5 and 11 in turn.

For the 2-subgroups, the number must be congruent to 1 modulo 2 and divide 55. Thus there could be 1, 5, 11 or 55 such subgroups.

For the 5-subgroups, the number must be congruent to 1 modulo 5 and divide 22. Thus there could be 1 or 11 such subgroups.

For the 11-subgroups, the number must be congruent to 1 modulo 11 and divide 10. Thus there can only be one such subgroup.

Hence we can be sure that there is a unique Sylow 11-subgroup, which is normal because it is unique. Since it has order 11, this subgroup is non-trivial. Since its order is less than that of the group, it is proper.

Solution to Exercise 2.8

The order factorises into primes as

$$132 = 2^2 \times 3 \times 11.$$

By the usual argument, the possibilities for the numbers of each type of Sylow subgroup are shown in the table below.

Sylow 2-subgroups	1, 3, 11 or 33
Sylow 3-subgroups	1, 4 or 22
Sylow 11-subgroups	1 or 12

We want to rule out the possibility that there is more than one of every Sylow subgroup type. Suppose that we have twelve Sylow 11-subgroups, at least four Sylow 3-subgroups and at least three Sylow 2-subgroups.

Since the Sylow 11-subgroups are cyclic of prime order, the twelve subgroups account for the identity element plus 120 elements of order 11. A similar argument shows that the four Sylow 3-subgroups, which are cyclic, account for eight non-identity elements, each of order 3.

We have accounted for 129 elements of the group: the identity, 120 elements of order 11 and eight elements of order 3. There are only three elements left, and these must be the three non-identity elements of a Sylow 2-subgroup (which has order 4). This contradicts the assumption

that there are at least three Sylow 2-subgroups. Thus at least one Sylow subgroup must be unique and hence normal, and so G is not simple.

Solution to Exercise 3.1

(a) From the presentation, we know that a has order 4, so

$$\langle a \rangle \cong \mathbb{Z}_4$$

is a cyclic subgroup of order 4.

(b) Let $H = \{e, a^2, b, a^2b\}$.

Closure is almost immediate. Probably the only combinations needing more than a mental check are the following:

$$\begin{aligned} ba^2 &= (a^3)^2 b \qquad \text{(since } ba = a^3b\text{)} \\ &= a^6 b \\ &= a^2 b; \end{aligned}$$

$$\begin{aligned} ba^2b &= (a^2b)b \qquad \text{(by the above)} \\ &= a^2b^2 \\ &= a^2; \end{aligned}$$

$$\begin{aligned} a^2ba^2 &= a^2(a^2b) \qquad \text{(by the above)} \\ &= a^4 b \\ &= b. \end{aligned}$$

The identity element is in H and each element is self-inverse (see below). Thus H is a subgroup.

The element a^2 is a half-turn, while the other two non-identity elements are reflections. Hence all non-identity elements are of order 2, so H must be isomorphic to the Klein group.

Solution to Exercise 3.2

(a) We have

$$\begin{aligned} |X| &= \frac{24 \times 23 \times 22 \times 21}{4 \times 3 \times 2 \times 1} \\ &= \frac{6 \times 23 \times 11 \times 21}{1 \times 3 \times 1 \times 1} \\ &= 2 \times 23 \times 11 \times 21 \, (= 10626). \end{aligned}$$

(b) From the factorisation in part (a), we can see that the highest power of 2 that divides $|X|$ is $2^1 = 2$.

(c) This time we have

$$\begin{aligned} |Y| &= \frac{24 \times 23}{2 \times 1} \\ &= 12 \times 23 \, (= 276). \end{aligned}$$

(d) The highest power of 2 that divides $|Y|$ is 2^2.

Solution to Exercise 3.3

We have $196 = 2^2 \times 7^2$. Thus the group has subgroups of order 7 and $7^2 = 49$.

Suppose that there are m subgroups of order 49. Then

$$m \equiv 1 \,(\mathrm{mod}\ 7) \quad \text{and} \quad m \mid 4.$$

Hence $m = 1$, so the Sylow 7-subgroup, of order 49, is unique and, hence, normal.

The abelian group $\mathbb{Z}_4 \times \mathbb{Z}_7 \times \mathbb{Z}_7$ has distinct subgroups

$$\{0\} \times \mathbb{Z}_7 \times \{0\} \quad \text{and} \quad \{0\} \times \{0\} \times \mathbb{Z}_7,$$

both of which have order 7.

Solution to Exercise 4.1

Since K is contained in the centre of G, we know that

$$kg = gk$$

for all $k \in K, g \in G$. In particular, $kh = hk$ for all $k \in K$ and $h \in H$, so we can apply Proposition 1.9(b) of Chapter 6 to conclude that HK is a subgroup of G and that

$$HK \cong H \times K.$$

Then Proposition 1.9(a) tells us that $|HK| = |H||K|$; hence, by condition 2, we have that

$$|G| = |HK|.$$

It follows that $G = HK$, hence $G \cong H \times K$ as required.

Solution to Exercise 4.2

If ϕ is a one–one homomorphism, to show that it is an isomorphism we just need to show that ϕ is onto.

Since ϕ is one–one, we know that

$$\phi(g_1) = \phi(g_2) \Rightarrow g_1 = g_2$$

for all $g_1, g_2 \in G$. Thus

$$|\{\phi(g) : g \in G\}| = |G| = |H|.$$

As $\{\phi(g) : g \in G\} \subseteq H$, this means that $\{\phi(g) : g \in G\} = H$ and so ϕ is onto as required.

Solution to Exercise 4.3

Let h be a generator of H, so $H = \langle h \rangle$ and h has order p^2. Then $\phi(h) = h^r$ for some integer r with $0 \leq r < p^2$.

Since ϕ^2 is the identity, we have that

$$h = \phi^2(h) = \phi(\phi(h)) = \phi(h^r) = [\phi(h)]^r = (h^r)^r = h^{r^2}.$$

Thus $h^{r^2-1} = e$ and, since $|h| = p^2$, we have that p^2 divides

$$r^2 - 1 = (r-1)(r+1).$$

It follows that p divides $r^2 - 1 = (r-1)(r+1)$ and, since p is prime, that either p divides $r-1$ or p divides $r+1$.

Suppose that p divides $r-1$. Then p does not divide $r+1$ (as p is an odd prime) and so neither does p^2. By Euclid's Lemma (Book A, Chapter 1, Theorem 4.12), we have that p^2 divides $r-1$. Then

$$r = kp^2 + 1 \quad \text{for some } k \in \mathbb{Z}.$$

The condition $0 \leq r < p^2$ forces $k = 0$, so $r = 1$, and therefore $\phi(h) = h$. Since h generates H, it follows that ϕ is the identity on H.

Now suppose that p divides $r+1$. Then p^2 divides $r+1$, again by Euclid's Lemma, so

$$r = kp^2 - 1 \quad \text{for some } k \in \mathbb{Z}.$$

Now the condition $0 \leq r < p^2$ forces $k = 1$, so that $r = p^2 - 1$. Since h has order p^2,

$$\phi(h) = h^{p^2-1} = h^{-1}.$$

Let $g \in H$. Since h generates H, we have $g = h^s$ for some $s \in \mathbb{Z}$, so

$$\phi(g) = \phi(h^s) = [\phi(h)]^s = (h^{-1})^s = h^{-s} = g^{-1}.$$

Solution to Exercise 4.4

(a) By Sylow's First Theorem, the subgroup H has order p^2. Then H has index 2 in G, and so it is normal (see Exercise 3.3(b) of Chapter 5).

Since H has order p^2, it is abelian by Theorem 2.15 of Chapter 7. Thus by Theorem 3.19 of Chapter 6, either $H \cong \mathbb{Z}_{p^2}$ or $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(b) Since H is normal in G, we have $|G/H| = 2$. The natural homomorphism $\theta\colon G \to G/H$ is defined by

$$g \mapsto gH \quad \text{for all } g \in G.$$

Let $x \in G$ and $x \notin H$. Then $\theta(x) \neq H$, otherwise we would have $xH = H$, that is $x \in H$. Therefore $\theta(x)$ does not have order 1, so it has order 2.

By Exercise 4.11(b) of Chapter 5, the order of $\theta(x)$ divides the order of x and so, as p is an odd prime, x cannot have order p.

(c) Since 2 is prime and divides the order of G, by Sylow's First Theorem we know that G has at least one Sylow 2-subgroup. As 2^n does not divide $|G|$ for $n \geq 2$, this subgroup must have order 2 and thus it is isomorphic to $\mathbb{Z}_2$. The non-identity element a in this subgroup has order 2. Thus $a^{-1} = a$.

Since H is normal in G, for $h \in H$ we have

$$\phi(h) = aha = aha^{-1} \in H,$$

so the image set of H under ϕ is H itself.

Next note that for any $h_1, h_2 \in H$,

$$\phi(h_1h_2) = ah_1h_2a = ah_1aah_2a = \phi(h_1)\phi(h_2).$$

This shows that ϕ is a homomorphism.

To see that ϕ is one–one, let $h_1, h_2 \in H$ be such that $\phi(h_1) = \phi(h_2)$. Then

$$\phi(h_1) = \phi(h_2) \Rightarrow ah_1a = ah_2a \Rightarrow h_1 = h_2.$$

The solution to Exercise 4.2 and the fact that $\phi(H) = H$ ensure that ϕ is onto H, and so it is an automorphism of H.

(d) Since H has index 2, it has two cosets. Since $a \notin H$, the two cosets are H and aH. Thus $G = aH \cup H$. For $h_1, h_2 \in H$, we have

$$ah_1ah_2 = ah_1\phi(h_2)a = \phi(h_1\phi(h_2)).$$

(e) Let ϕ be the homomorphism defined in part (c), and observe that for all $h \in H$,

$$\phi^2(h) = \phi(aha) = a^2ha^2 = h.$$

Therefore ϕ^2 is the identity map on H. By the solution to Exercise 4.3, the automorphism $\phi : H \to H$ satisfies either $\phi(h) = h$ for all $h \in H$ or $\phi(h) = h^{-1}$ for all $h \in H$.

If $\phi(h) = h$ for all $h \in H$, then $aha = h$ for all $h \in H$. We know from part (d) that $G = aH \cup H$, so this implies that G is abelian. Then Theorem 2.2 gives $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$. Since p is an odd prime, Theorem 2.11 of Chapter 6 gives $G \cong \mathbb{Z}_{2p^2}$.

If G is not abelian then G has presentation

$$G = \langle a, h \mid a^2 = e, h^{p^2} = e, aha = h^{-1} \rangle,$$

so $G \cong D_{p^2}$.

(f) By the Sylow Theorems (Theorem 1.12), the number of Sylow 2-subgroups is odd and divides $2p^2$. Thus there are $1, p$ or p^2 subgroups of order 2.

The required result follows since each Sylow 2-subgroup contains exactly one element of order 2.

(g) If G has exactly one element of order 2, then there is a unique Sylow 2-subgroup K, say, and this is normal.

Since p is an odd prime, $K \cap H = \{e\}$. Now both H and K are normal subgroups of G. Moreover $|H||K| = |G|$, so $G = HK$. Then Theorem 1.5 of Chapter 6 gives

$$G \cong H \times K.$$

Since H and K are abelian, so is G by Exercise 1.4 of Chapter 6. Thus G is isomorphic to one of $\mathbb{Z}_{2p} \times \mathbb{Z}_p$ and $\mathbb{Z}_{2p^2}$.

(h) Suppose that G has p elements of order 2.

If $H \cong \mathbb{Z}_{p^2}$ then, by part (e), either $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ or $G \cong D_{p^2}$.

If $G \cong \mathbb{Z}_2 \times \mathbb{Z}_{p^2}$ we know G has one element of order 2. If $G \cong D_{p^2}$, we know G has p^2 elements of order 2 (corresponding to the reflections). Both cases contradict the assumption that G has p elements of order 2. It follows that $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Note that this means that all non-identity elements of H have order p.

Let $a \in G$ with $a^2 = e$. Then $G = H \cup aH$ by part (d). Since no elements of H have order 2, there is $h \in H,\ h \neq e$ such that $(ah)^2 = e$. Then

$$aha = h^{-1}.$$

Let K be the subgroup of G generated by a and h. Then

$$K = \{a^m h^n : a^2 = e, h^p = e, aha = h^{-1}\};$$

that is, $K \cong D_p$.

Let $g \in H$ but $g \notin \langle h \rangle$. Then $\langle g \rangle$ and $\langle h \rangle$ are subgroups of H of order p with trivial intersection. Since H is abelian,

$$H \cong \langle g \rangle \times \langle h \rangle,$$

and $h_1 g h_1^{-1} = g$ for all $h_1 \in H$.

Now consider the element a of order 2. Since $g \in H$ and H is normal in G, we know $aga \in H$. Then the decomposition of H as $\langle g \rangle \times \langle h \rangle$ gives

$$aga = (g^r, h^s) \quad \text{for some } r, s \in \mathbb{Z}.$$

But a has order 2, therefore

$$(g, e) = g = a(aga)a = (ag^r a, ah^s a).$$

Now $ah^s a = e \Rightarrow h^s = e$ and $ag^r a = g \Rightarrow g^r = g$, using left and right cancellation. Thus $aga = (g, e) = g$. We have shown that g is central in G and so $\langle g \rangle$ is in the centre of G.

Then the solution to Exercise 4.1 gives

$$G \cong \langle g \rangle \times K \cong \mathbb{Z}_p \times D_p\,.$$

(i) Suppose that $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and that G has p^2 elements of order 2. Let a be an element of order 2. Then $G = H \cup aH$ by part (d).

Since $|aH| = p^2$ and since no elements of H have order 2, the product ah has order 2 for all $h \in H$. Thus $ahah = e$ for all $h \in H$, that is, $aha = h^{-1}$. Therefore for $h_1, h_2 \in H$ we have

$$ah_1 ah_2 = h_1^{-1} h_2.$$

We now have enough information to construct a Cayley table for G and so have determined G up to isomorphism.